# 新手学黑客攻防

神龙工作室 编著


立体化视频教学光盘

本书适合你吗？

- 如果你是第一次接触黑客知识
- 如果你想让电脑更加安全
- 如果你不希望被他人窥探隐私

畅销经典

我的第1本黑客攻防入门书

200万读者的共同选择

人民邮电出版社
POSTS & TELECOM PRESS


**三维一体的学习套餐**

**让你轻松学得会**

封面设计：董志桢

分类建议：计算机／基础入门

人民邮电出版社网址：www.ptpress.com.cn

ISBN 978-7-115-24521-2

ISBN 978-7-115-24521-2

定价：29.80 元

附光盘+黑客工具软件速查手册

# 前　言

毋庸置疑，互联网已经深入人们日常生活和工作的各个角落，人们在享受网络带来的便利的同时，多数网民都在面临着不同程度的网络安全的威胁。很多人对黑客攻防感到“畏惧”，觉得其过于复杂，他们基本不懂如何让电脑更安全，或者如何能有效防范黑客的攻击。

黑客攻防真的这么难学吗？

## 本书适合谁阅读

如果您是第一次接触黑客知识；如果您希望电脑免遭黑客攻击；如果您确实想学习黑客攻防知识但认为其很难学；如果您对黑客攻防知识一知半解，只会一些简单的操作。这 4 项假设，只要您符合一项，那么本书就是为您量身定制的，您可以在阅读中找到将本书翻烂的理由。

## 为什么要阅读本书

历时 8 年，获得无数读者与书店工作人员的称赞，并创下 200 万册销量奇迹的“新手学”系列图书，是值得信赖的图书品牌；根据初学者的阅读习惯、学习需求，安排章节与内容，让您学习黑客攻防“零障碍”；随书附带情景互动式多媒体教学光盘，细致入微地引导您学习黑客攻防的全过程。

无论您是要立志成为一名专业的电脑安全人士，还是仅在日常工作、生活中用来让自己的电脑更安全，本书都将给您带来贴心的阅读体验。

从黑客攻防基础知识的介绍到能够熟练地使用，从设置电脑安全策略到使用安全工具防范黑客攻击，从黑客工具的打开方法到了解黑客是如何进行信息的收集、扫描和攻击，本书都将娓娓道来。本书还融入培训师、网络安全专家多年的实践经验，可以让您在学习过程中少走弯路。阅读完本书，您会发现：黑客攻防真的不难学！

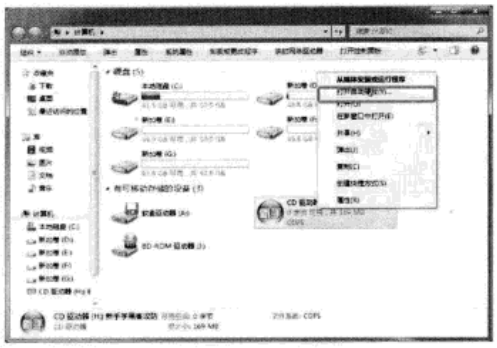
## 您将从本书学到什么

深入了解电脑，从而了解黑客攻击电脑的原理，以及黑客使用的基本命令
了解黑客常用工具的使用方法
掌握典型的黑客攻防技巧
掌握电脑安全策略的设置方法
掌握使用端口、漏洞等扫描工具和控制工具进行信息的收集、扫描的方法
掌握使用防木马软件、防火墙和杀毒软件等来防范黑客攻击的方法

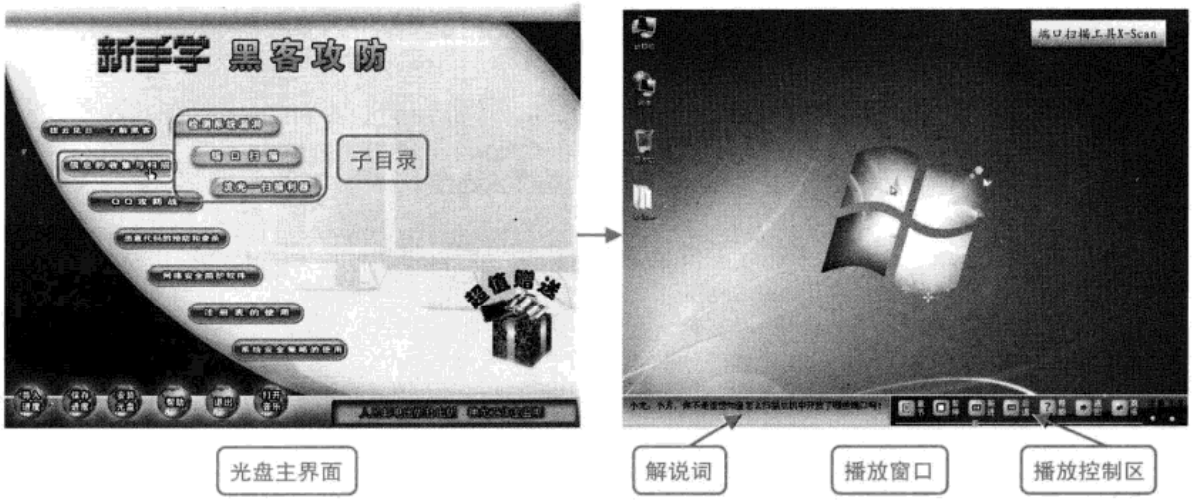
## 光盘使用说明

本书附带一张多媒体电脑教学光盘。

（1）将光盘印有文字的一面朝上放入光驱中，几秒钟后光盘就会自动运行。若光盘没有自动运行，可以打开【计算机】窗口，然后在光盘图标上单击鼠标右键，从弹出的快捷菜单中选择【打开自动播放】菜单项，光盘就会运行。



（2）稍后会进入光盘的主界面，此时可以看到光盘中包含的各个章节目录，将鼠标指针移到目录按钮上并单击鼠标左键，弹出对应的下一级子目录，然后单击某个子目录按钮即可进入光盘的播放界面，并自动播放该节的内容。




## 光盘内容介绍

进入光盘主界面之后，可通过单击主界面中的按钮，有选择地学习光盘中的内容。光盘的主要内容介绍如下。

- 了解黑客是如何攻击电脑的，以及黑客常用的攻击方式和常用命令。
- 介绍信息的收集与扫描的方法，介绍 QQ 攻击和防御的方法。
- 介绍恶意代码的预防和查杀方法。
- 介绍网络安全防护软件的使用方法。
- 介绍注册表和系统安全策略的使用方法。
- 赠送 400 招 Windows 7 实用技巧。

本书由神龙工作室编写，若您在阅读过程中遇到困难或疑问，可以给我们写信，本书责任编辑的联系邮箱：maxueling@ptpress.com.cn。

编 者

# 目 录 Content

## 第 3 章



系统会将用户在使用电脑过程中的操作记录下来，这样方便了用户查阅以前的操作，但这些记录往往也会成为网络攻击者利用的漏洞。



## 第 4 章

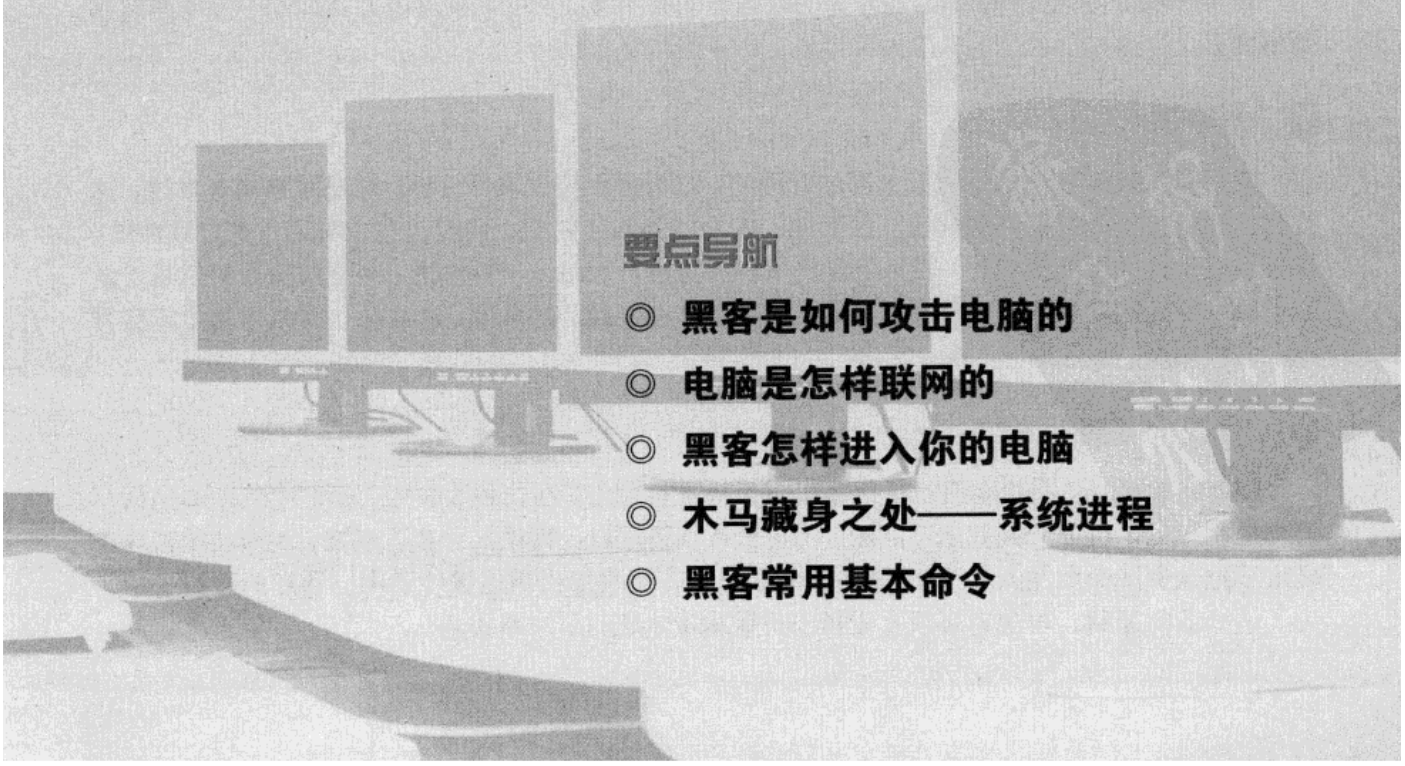


黑客一般通过系统漏洞和远程控制技术对用户电脑进行攻击和控制，在此过程中，密码起着重要的防范作用。

# 第1章

# 拨云见日——了解黑客

一提起黑客，人们总感到他们身上带有一种神秘的色彩，仿佛是不可琢磨、难以接近的高超人物。黑客到底扮演着什么样的角色呢？也许是网络里潜伏的杀手，也许是在攻入用户系统后提醒用户其系统漏洞所在并留下建议便悄然离去的侠士……



## 要点导航

- ◎ 黑客是如何攻击电脑的
- ◎ 电脑是怎样联网的
- ◎ 黑客怎样进入你的电脑
- ◎ 木马藏身之处——系统进程
- ◎ 黑客常用基本命令

# 1.1 黑客是如何攻击电脑的

人们总会将黑客和破坏网络安全、盗取网络密码等联系在一起，感到他们非常神秘。那么他们到底是一群什么样的人？他们从事什么活动呢？

## 1. 黑客的由来

黑客，又称为骇客，源于英文单词Hacker。原意是指那些精通操作系统和网络技术，并利用其专业知识编制新程序的人。他们往往都精通计算机和网络知识，除了无法通过正当的手段物理性地破坏他人的计算机和帮助他人重装操作系统外，其他的绝大部分的计算机操作他们都可以通过网络做到，如监视他人计算机、入侵网站服务器替换该网站的主页、攻击他人计算机、盗取计算机中的文件等。

随着网络技术的发展和黑客工具的传播，一些人开始利用黑客工具对一些疏于防范的计算机进行攻击、破坏，例如，监视他人计算机、偷窥他人隐私、盗取用户资料、入侵网络服务器等。这就不属于黑客的范畴，而是犯罪活动。在日常生活中，许多网络安全故障也都出自黑客之手，如某些网站无法访问、网上银行账户被盗等。

目前，世界上有很多黑客网站，这些网站会介绍一些常用的黑客知识和系统的一些漏洞，并免费提供一些常用的软件供网友下载使用。现在，黑客技术已经被越来越多的人掌握，对于普通的计算机用户来说，了解常用的黑客技术，有助于更好地保护自己的计算机免受恶意攻击。

## 2. 常见的黑客攻击方式

黑客的攻击方式多种多样，但常见的攻击方式并不多，以下几种攻击方式基本上每个黑客都会用到。

### ○ 网络报文嗅探

网络嗅探其实最开始是应用于网络管理的，就像远程控制软件一样，但随时被黑客发现，这些强大的功能就开始被黑客利用。最普遍的安全威胁来自内部，同时这些威胁通常都是致命的，其破坏性也远大于外部威胁。很多黑客使用嗅探器进行网络入侵的渗透。网络嗅探器对信息安全的威胁来自其被动性和非干扰性，使得网络嗅探具有很强的隐蔽性，这往往让网络信息泄露变得不容易被发现。

### ○ IP 地址欺骗

IP地址欺骗攻击是黑客假冒受信主机对目标进行攻击。在这种攻击中，受信主机指的是拥有管理控制权的主机或明确做出“信任”决定允许其访问自己网络的主机。通常，IP地址欺骗攻击局限于把数据或命令注入客户机/服务器应用之间，或对等网络连接传送中已存在的数据流中。为了达到双向通信，攻击者必须改变指向被欺骗IP地址的所有路由表。

### 拒绝服务攻击

拒绝服务（Denial of Service，DoS）攻击是目前最常见的一种攻击类型。从网络攻击的各种方法和所产生的破坏情况来看，DoS是一种简单有效的攻击方式。它的目的就是拒绝用户的服务访问，破坏网络的正常运行，最终使用户的网络连接阻塞，或者服务器因疲于处理攻击者发送的数据包而使服务器系统的相关服务崩溃、系统资源耗尽。这类攻击和其他大部分攻击不同的是，因为它们不是以获得网络或网络上信息的访问权为目的，而是要使受攻击方耗尽网络、操作系统或应用程序有限的资源而崩溃，不能为其他用户提供服务。这就是这类攻击被称为“拒绝服务攻击”的原因。

### 应用层攻击

应用层攻击可以使用多种不同的方法来实现，最常用的方法是利用服务器中的应用软件（如SQL Server、Sendmail、PostScript和FTP）的缺陷。通过使用这些缺陷，攻击者能够获得计算机的访问权，以及该计算机上运行相应应用程序所需的账户。

## 1.2 电脑是怎样联网的

每台电脑都拥有全球唯一的MAC地址（物理地址）。人们为了区分网络中的主机又为联网的每台电脑分配了一个IP地址。

### 1.2.1 认识IP地址

IP地址就是人们为了区分网络中的主机，为每台主机分配的一个专门地址。

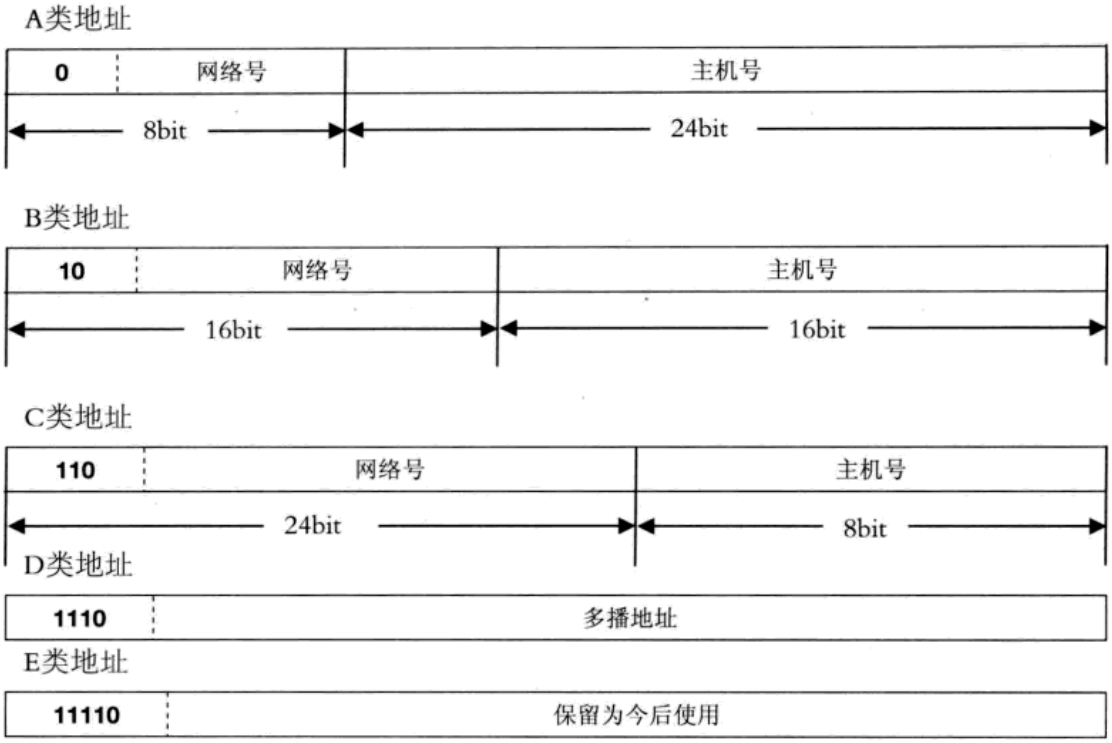
### IP 地址的表示方法

IP地址由4字节组成，每字节对应8位二进制位（即每部分数字不会超过$2^8$=256），例如，采用二进制形式记录的某个IP地址可以表示为“00010110001011001001000010101”。为了方便使用，IP地址的每字节通常被写成十进制的形式，中间用“.”分隔，这样就可以用XXX.XXX.XXX.XXX的形式来表示，其中，每组“XXX”代表不大于255的十进制数。例如，上面的IP地址就可以表示为11.11.36.21。IP地址的这种表示方法称为“点分十进制表示法”，这显然比二进制的1和0更容易记忆。

### IP 地址的分类

一般情况下，可以将IP地址分为五大类。

IP地址的分类如下图所示。




A类地址以第一字节为网络号，其中第一位为0，其范围为1.0.0.1~126.255.255.254，另外，保留127.0.0.1~127.255.255.254地址段用于本地软件的环回测试，例如，127.0.0.1就是指本机；B类地址以前两字节为网络号，其中第一字节的前两位必须是10，其范围为128.0.0.1~191.255.255.254；C类地址以前三字节为网络号，其中第一字节的前三位必须是110，其范围为192.0.0.1~233.255.255.254；D类地址不分网络号和主机号，它的第一字节的前四位固定为1110，其范围为244.0.0.1~239.255.255.254，D类地址用于多播通信（一对多通信），主要留给因特网体系结构委员会IAB（Internet Architecture Board）使用；E类地址不分网络号和主机号，它的第一字节的前五位为11110，其范围为240.0.0.1~255.255.255.254，E类地址保留为以后使用。

A类地址中的地址段10.0.0.0~10.255.255.255、B类地址中的地址段172.16.0.0~172.31.255.255和C类地址中的地址段192.168.0.0~192.168.255.255等作为私有地址，不能用在互联网上，而只能用于局域网。

另外，全零地址（0.0.0.0）指任意网络。全“1”的IP地址（255.255.255.255）是指当前子网的广播地址。

## 1.2.2 认识MAC地址

MAC（Medium/Media Access Control，介质访问控制）地址，用来定义网络设备的位置。在OSI参考模型中，第三层网络层负责IP地址，第二层数据链路层则负责MAC地址。因此一个主机

会有一个IP地址，而每个网络位置都会有一个专属于它的MAC地址。

## 什么是 MAC 地址

MAC地址，也叫硬件地址，是由48比特（6字节）长，十六进制的数字组成，是识别LAN（局域网）节点的标识。

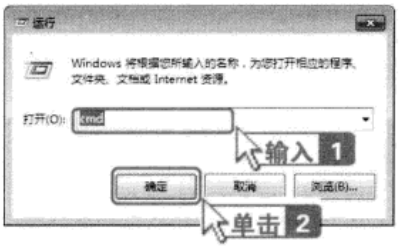
MAC地址在网卡里。网卡的物理地址通常由网卡生产厂家写入网卡的EPROM（一种闪存芯片，通常可以通过程序擦写）中，它存储的是传输数据时真正用于标识发出数据和接收数据的主机的地址。

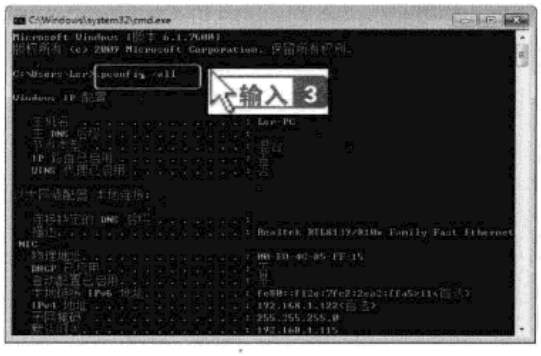
MAC地址就如同身份证号码，具有全球唯一性。

## 如何获取本机 MAC 地址

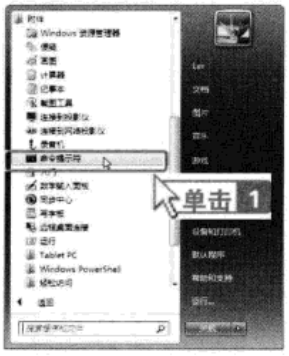
在Windows 7操作系统中，获取本机MAC地址的方法通常有以下3种。

第一种：单击【开始】➢【运行】菜单项，在弹出的【运行】对话框的【打开】下拉列表中输入“cmd”，并单击 确定 按钮，弹出【C:\Windows\system32\cmd.exe】窗口，在该窗口中输入“ipconfig /all”，然后按下【Enter】键即可查看本机的MAC地址。



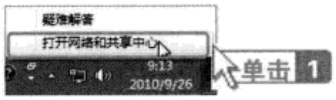



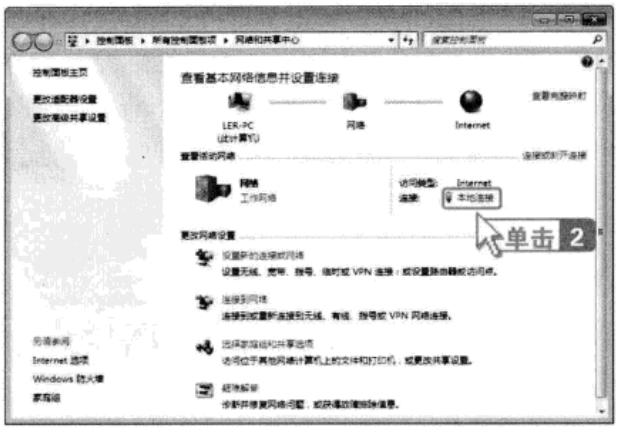

第二种：依次单击【开始】➢【所有程序】➢【附件】➢【命令提示符】菜单项，在弹出的【命令提示符】窗口中输入“ipconfig /all”，然后按下【Enter】键即可。




第三种：通过查看本地连接获取MAC地址。具体的操作步骤如下。

步骤1 在桌面的右下角右键单击【网络Internet访问】按钮，在弹出的快捷菜单中选择【打开网络和共享中心】菜单项，弹出【网络和共享中心】窗口，接着单击【查看活动网络】组合框中的【本地连接】链接。




步骤2 弹出【本地连接 状态】对话框，单击 详细信息(E)... 按钮，在弹出的【网络连接详细信息】对话框中查看MAC地址即可。



## 1.3 黑客怎样进入你的电脑

端口是计算机与外界进行通信交流的出口。黑客也正是通过端口进出用户电脑的。

### 1.3.1 黑客进出的门户——端口

端口是黑客进出电脑的门户，主要分为硬件端口和软件端口两种。其中硬件端口又称为接口，分为串行接口和并行接口两种。串行接口主要有USB、SATA和IDE等，平常使用的打印机接口就属于并行接口。软件端口一般指网络中面向连接服务和无连接服务的通信协议端口，是一种抽象

的软件结构，包括一些数据结构和I/O（输入/输出）缓冲区。

在网络技术中，端口（Port）的含义有多种。集线器、交换机、路由器的端口指的就是连接其他网络设备的接口，如RJ-45端口、Serial端口等。这里所指的端口不是物理意义上的端口，而是特指TCP/IP中的端口，是逻辑意义上的端口。

端口用来解决主机应该把接收到的数据包传送给众多同时运行进程中的哪一个的问题。例如，http使用80号端口，FTP使用21号端口，这样通过不同的端口，电脑同时运行的不同程序就可以互不干扰地进行通信了。通常来说，一台电脑一般有65 535个端口，但常用的端口只有几十个，由此可见，还有大量的端口没有使用。这样，黑客程序就可以采用某种方法，打开没有使用的端口，从而对电脑进行控制。

## 1.3.2 常用的电脑端口

计算机中的65 535个端口按不同的分类标准可以分为很多类，其中最常用的分类标准有按端口号和协议类型分类两种。

### 1. 按端口号分类

按端口号可以将电脑中的端口分为3类，分别是“公认端口”、“注册端口”和“动态和/或私有端口”。

#### ● 公认端口

公认端口（Well Known Ports）也称为“常用端口”，其端口号的范围为0~1 023，它们紧密地绑定于一些特定的服务。通常这些端口的通信明确地表明了某种服务的协议，这种端口不可再重新定义它的作用对象。例如，21端口分配给了FTP服务，而23端口是Telnet服务专用的，SMTP使用25号端口，80端口是HTTP通信所使用的，135端口分配给了RPC（远程过程调用）服务，这些端口通常不会被如木马这样的黑客程序利用。

#### ● 注册端口

注册端口（Registered Ports）的端口号范围为1 024~49 151，它们松散地绑定于一些服务。也就是说有许多服务绑定于这些端口，这些端口同样用于许多其他的目的。这些端口大多数没有明确定义的服务对象，应用程序会根据自己的实际需要进行定义。例如，腾讯QQ客户端用的就是4000端口。需要指出的是：这些端口也是木马程序的常用端口，是防护和查杀木马程序必须要检查的端口。

#### ● 动态和/或私有端口

动态和/或私有端口（Dynamic and/or Private Ports）的端口号范围为49 152~65 535。理论上

不应将这些端口分配给服务，但实际上一些较为特殊的程序，特别是一些木马程序就喜欢使用这些端口，因为这些端口通常不被人们注意，容易隐藏。

### 2. 按协议类型分类

端口的另一种分类标准是按协议类型分类。网络上常用的通信协议有两种，分别是面向连接的TCP（传输控制协议）和面向无连接的UDP（用户数据报协议），对于这两种通信协议的服务所提供的端口，可以将计算机端口分为TCP端口和UDP端口。由于TCP和UDP是相互独立的，因此它们各自的端口号也相互独立，例如，TCP使用235号端口，UDP也可以使用235号端口，这两者是不冲突的。

#### 使用 TCP 的常见端口

(1) FTP

FTP（文件传输协议）使用21号端口，主要用于文件传输服务，例如上传和下载文件。

(2) Telnet协议

Telnet（远程登录）协议使用23号端口，用户可以以自己的身份连接到远程计算机上。

(3) SMTP

SMTP（简单邮件传输）使用25号端口，大多数的邮件服务器都采用这个协议，用于发送邮件。

(4) POP3

POP3和SMTP相对应，用于接收邮件，通常情况下使用的是110号端口。

#### 使用 UDP 的常见端口

(1) HTTP

HTTP（超文本传输协议）是用户使用最多的协议。上网浏览网页时就是使用这个协议，提供HTTP服务需要开启80号端口。

(2) DNS协议

DNS协议用于域名解析服务，由于IP地址是纯数字形式的，不方便记忆，于是就出现了便于记忆的域名，但计算机只能通过IP地址寻找要访问的主机，此时就需要将域名解析成IP地址，将域名解析成IP地址的工作就是由DNS服务器来完成的，该服务使用53号端口。

(3) SNMP

SNMP（简单网络管理协议）使用161号端口，主要用来管理网络设备。

(4) QQ

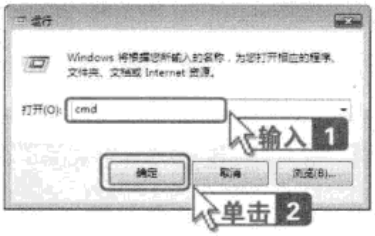
QQ客户端既可以发送信息又可以接收信息，其采用的协议是UDP。它使用8000号端口侦听是否有数据到来，使用4000号端口向外发送数据。

### 1.3.3 查看电脑端口的命令

在Windows 2000/XP/Server 2003/Vista/Server 2008/7中，可以使用netstat命令来查看活动端口的情况。具体的操作步骤如下。

步骤1 单击【开始】➢【运行】菜单项，在弹出的【运行】对话框中的【打开】下拉列表中输入“cmd”命令，然后单击 确定 按钮。

步骤2 在弹出的【C:\Windows\system32\cmd.exe】窗口中输入“netstat /a /n”命令，按下【Enter】键，即可看到以数字形式显示的活动的TCP连接和UDP连接的端口号以及状态。





如果想对某台电脑进行攻击，必须对目标电脑的情况有大概的了解，这时可以用扫描工具对目标主机进行扫描。这样就可以得到目标主机打开端口的情况，进而推测出目标电脑提供了哪些服务，从而对目标电脑有初步的了解。

如果在管理员不知情的情况下计算机的端口打开得太多，那么可能有两种情况：一种是提供了服务而管理员没有注意，例如，安装IIS（Internet Information Server，因特网信息服务）时就会自动增加很多服务；二是电脑被安装了木马，通过一些特殊的端口进行通信。这都是很危险的，如果管理员不了解电脑提供的服务，就会降低系统的安全性。因此扫描本机开放端口是做好电脑安全防范的首要工作。

### 1.3.4 怎样关闭端口

在默认情况下，用户系统有很多没用的或者不安全的端口是开启的，这些端口很容易被黑客

利用，为了保证系统的安全，用户可以关闭一些不用的端口。

关闭端口的方式有很多种，可以通过关闭相应的服务来阻止访问，也可以通过限制相应的端口号来阻止访问。

### 1. 关闭相应服务阻止访问端口

计算机中的各项服务通常都对应相应的端口，例如，WWW服务对应80号端口，SMTP对应25号端口等，因此关闭相应的服务也就关闭了其对应的端口。

下面就以关闭Remote Desktop Services（远程桌面服务）为例进行介绍，具体的操作步骤如下。

步骤1 单击【开始】➢【控制面板】菜单项，弹出【控制面板】窗口，双击【管理工具】图标，在弹出的【管理工具】窗口中双击【服务】图标。



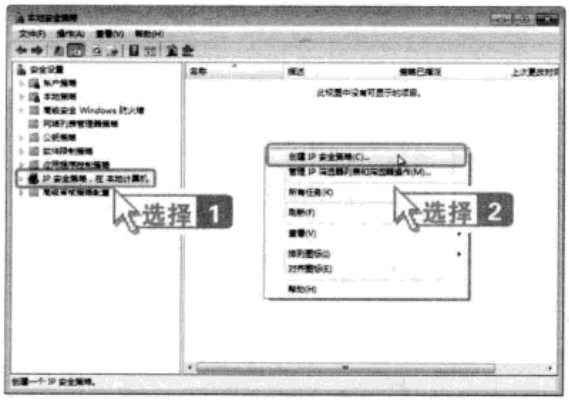
步骤2 弹出【服务】窗口，拖动窗口右侧的滚动条，找到Remote Desktop Services选项，然后双击该选项，打开【Remote Desktop Services的属性（本地计算机）】对话框，切换到【常规】选项卡，在【启动类型】下拉列表中选择【禁用】选项，然后单击 确定 按钮即可关闭该服务也就关闭了该服务对应的端口。


## 2. 限制端口的方法

通过限制访问指定的端口号，同样可以达到关闭端口的目的。下面以3389号端口为例进行介绍。

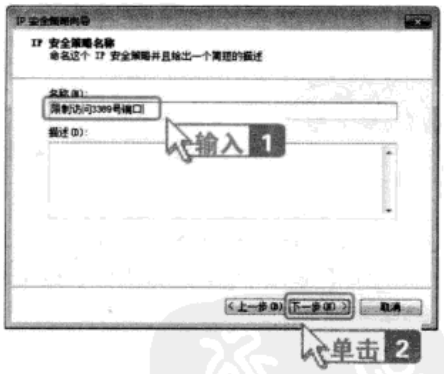
步骤1 打开【控制面板】窗口，双击【管理工具】图标，在弹出的【管理工具】窗口中双击【本地安全策略】图标。

步骤2 打开【本地安全设置】窗口，在左侧的窗格中选择【IP安全策略，在本地计算机】选项，接着在右侧窗格的空白处单击鼠标右键，从弹出的快捷菜单中选择【创建IP安全策略】菜单项。

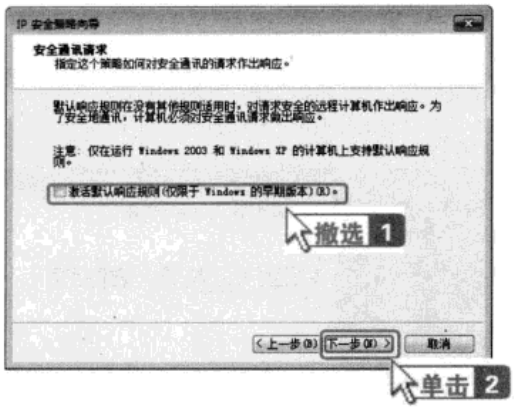



步骤3 打开【IP安全策略向导】对话框，然后单击下一步(N) >按钮。

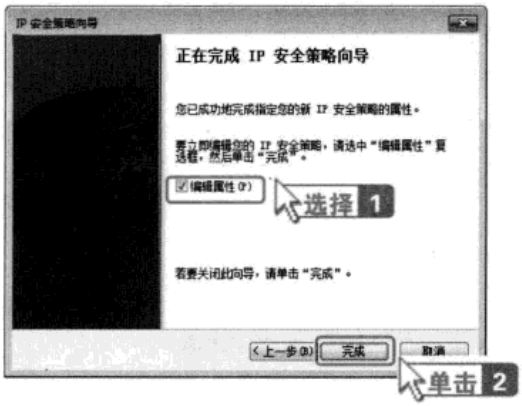

步骤4 打开【IP安全策略名称】对话框，在这里可以设置所创建的IP安全策略的名称和描述，这里在【名称】文本框中输入“限制访问3389号端口”，然后单击下一步(N) >按钮。




步骤5 弹出【安全通讯请求】对话框，指定这个策略对安全通讯的请求所作出的响应。这里取消选中【激活默认响应规则（仅限于Windows的早期版本）】复选框，然后单击下一步(N) >按钮。



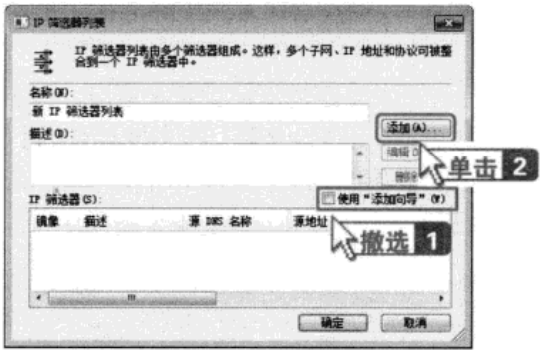

步骤6 打开【正在完成IP安全策略向导】对话框，选择【编辑属性】复选框，单击 完成 按钮。




步骤7 打开【限制访问3389号端口 属性】对话框，取消选中【使用“添加向导”】复选框，然后单击 添加(D)... 按钮。

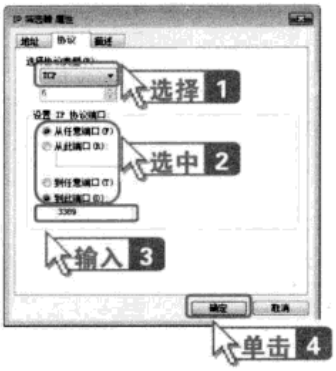

步骤8 弹出【新规则 属性】对话框，并单击 添加(D)... 按钮。


步骤9 打开【IP筛选器列表】对话框，取消选中【使用“添加向导”】复选框，单击 添加(A)... 按钮。



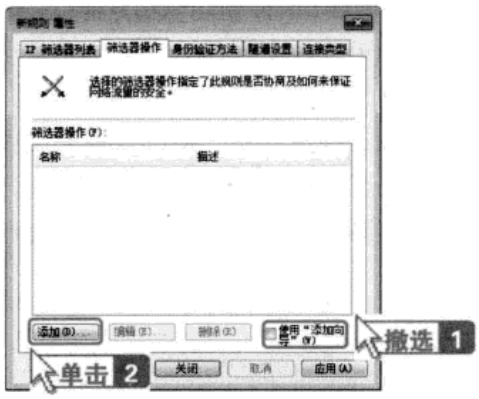

步骤10 打开【IP筛选器 属性】对话框，在【源地址】和【目标地址】下拉列表中分别选择【任何IP地址】和【我的IP地址】选项。

步骤11 切换到【协议】选项卡，在【选择协议类型】下拉列表中选择【TCP】选项，在【设置IP协议端口】组合框中选中【从任意端口】单选钮和【到此端口】单选钮，然后在【到此端口】下面的文本框中输入“3389”，最后单击 确定 按钮。

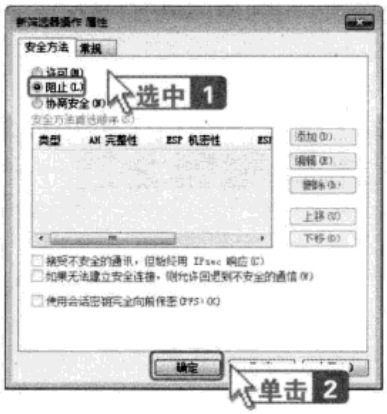



步骤12 返回【IP筛选列表】对话框，如果用户想要再添加几个限制端口，可以继续单击 添加(A)... 按钮进行添加，添加完成后单击 确定 按钮。返回【新规则 属性】对话框，在【IP筛选器列表】列表框中选中【新IP筛选器列表】单选钮。

步骤13 切换到【筛选器操作】选项卡，取消选中【使用“添加向导”】复选框，单击 添加(D)... 按钮。



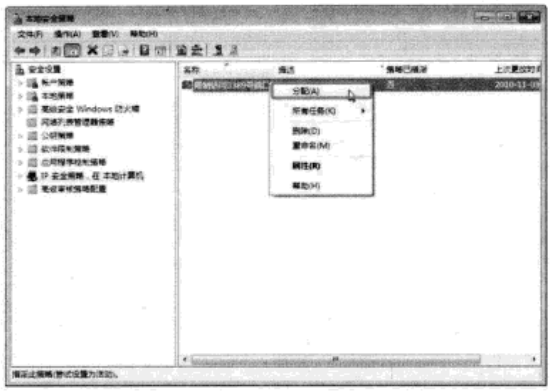

步骤14 打开【新筛选器操作 属性】对话框，切换到【安全方法】选项卡，选中【阻止】单选钮，然后单击 确定 按钮。




步骤15 返回【新规则 属性】对话框，选中【筛选器操作】列表框中的【新筛选器操作】单选钮，然后单击 关闭 按钮。

步骤16 返回【限制访问3389号端口 属性】对话框，用户可以发现在【IP安全规则】列表框中增加了一个【新IP筛选器列表】选项，并且其左边的复选框呈选中状态，单击 确定 按钮，即可添加一个限制访问3389号端口的IP安全策略。


步骤17 重新进入【本地安全设置】窗口中，并在右侧窗格中的【限制访问3389号端口】选项上单击鼠标右键，从弹出的快捷菜单中选择【分配】菜单项，最后重新启动计算机即可使设置生效。




## 1.4 木马藏身之处——系统进程

因为木马存在于系统中，所以无法彻底和系统进程脱离关系，即使采用了隐藏技术，也还是能够从系统进程中找到蛛丝马迹，因此，查看系统中活动的进程成为检测木马最直接的方法。

### 1.4.1 认识系统进程

系统进程是系统或应用程序的一次动态执行。简单地说，它是操作系统当前运行的执行程序。在系统中打开任何一个软件，系统便会在后台加载相应的进程。

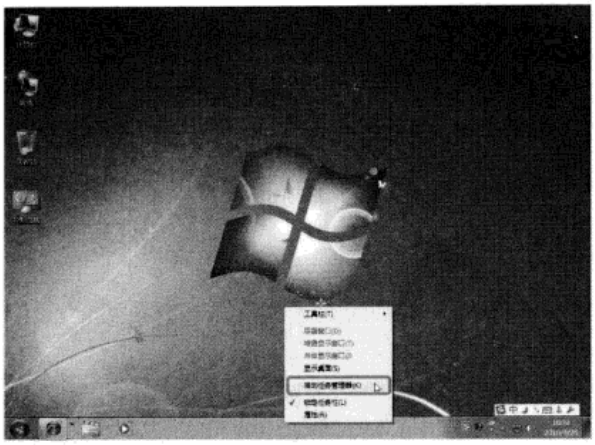
在系统当前运行的执行程序里包括：系统管理计算机个体和完成各种操作所必需的程序；还有用户开启、执行的额外程序，当然也包括用户不知道的、自动运行的具有重要作用的程序，正是因为进程具有这种特性，所以它也经常受到“入侵”。

### 1.4.2 打开系统进程

打开系统进程的方法非常简单。具体的操作步骤如下。

步骤1 在桌面的任务栏处单击鼠标右键，在弹出的快捷菜单中选择【启动任务管理器】选项。

步骤2 弹出【Windows任务管理器】窗口，切换到【进程】选项卡中即可查看系统进程。




另外，用户还可以利用快捷键打开系统进程。按下【Ctrl】+【Alt】+【Del】组合键，在弹出的界面中单击【启动任务管理器】按钮，然后在弹出的【Windows任务管理器】窗口中切换到【进程】选项卡即可。

## 1.4.3 关闭和新建系统进程

用户在进入【Windows任务管理器】窗口后，在【进程】选项卡中，可以对系统进程进行查看、关闭和新建等操作。

### 1. 关闭系统进程

要关闭系统进程，只需要选中相应的系统进程，然后单击窗口右下角的 结束进程(E) 按钮即可。


但是，在关闭某些系统进程时要注意，比如关闭explorer.exe进程，由于该进程用于管理Windows图形壳，包括【开始】菜单、任务栏、桌面和文件管理。删除该程序会导致Windows图

形界面无法使用，鼠标也没有响应。

### 2. 新建系统进程

下面以新建explorer.exe进程为例，介绍创建系统进程的操作步骤。

步骤1 按下【Ctrl】+【Alt】+【Del】组合键，打开【Windows任务管理器】窗口，切换到【进程】选项卡，在菜单栏中选择【文件】➢【新建任务（运行…）】菜单项。

步骤2 弹出【创建新任务】对话框，在【打开】下拉列表中输入“explorer.exe”，然后单击 确定 按钮即可。

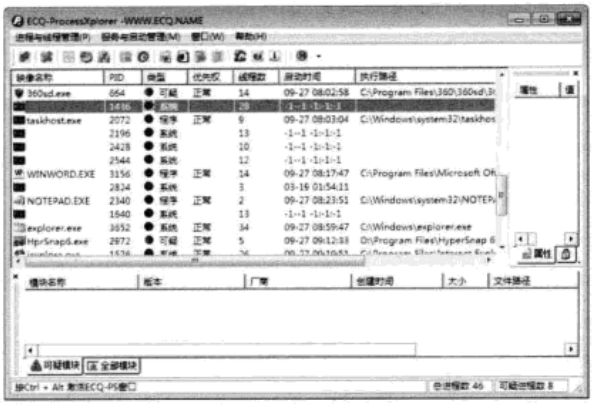


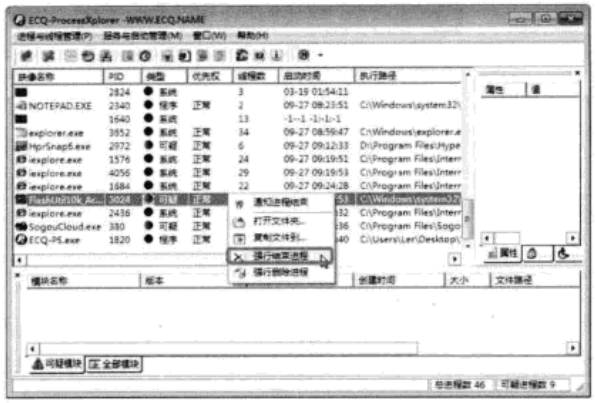
## 1.4.4 查看隐藏进程

查看隐藏进程的方法有很多，在这里使用“隐藏进程管理工具”，来完成对隐藏进程的查看和管理。具体的操作步骤如下。

步骤1 下载“隐藏进程管理工具”软件，双击“ECQ-PS.exe”文件，运行“隐藏进程管理工具”程序，在打开的窗口中可以看到系统中所有的进程。在每个进程后面，可以看到此程序的线程、主要关联的程序及其路径等内容。

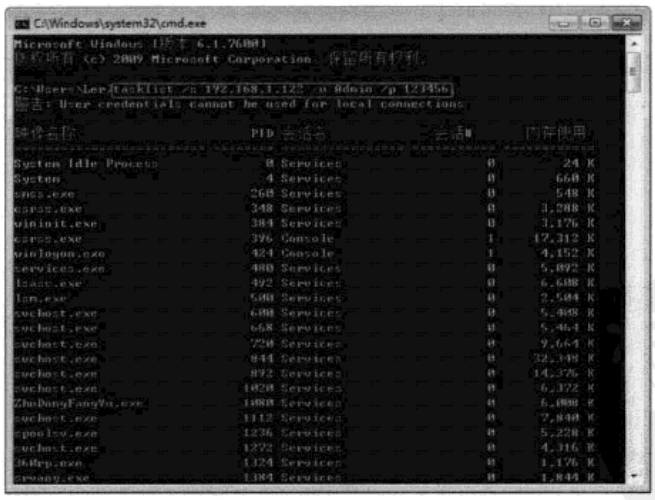
步骤2 对于提示为“可疑”的进程，在查看其文件路径后，当确认为恶意程序时，可以选中此进程并单击鼠标右键，在弹出的快捷菜单中选择【强行结束进程】菜单项即可。





## 1.4.5 查看远程进程

查看远程电脑的进程是黑客的基本功，也是他们经常干的事情，其方法很简单。具体的操作方法是：选择【开始】➢【运行】菜单项，在弹出的【运行】对话框中的【打开】下拉列表中输入“cmd”命令，然后单击 确定 按钮。在弹出的【命令提示符】窗口中输入“tasklist /s 192.168.1.122 /u Admin /p 123456”命令，按下【Enter】键，稍等片刻就可以得到远程电脑反馈回来的进程列表信息了。




其中“/s”参数后的“192.168.1.122”是指要查看远程系统的IP地址；“/u”参数后的“Admin”是指tasklist命令使用的用户账户；“/p”参数后的“123456”是指Admin账户的密码。

通过上面的命令可以得到远程电脑的进程列表，然后黑客就可以判断出自己植入的木马等程序是否在远程电脑上运行。

## 1.5 黑客常用基本命令

黑客使用的命令很多，掌握各种命令的使用方法是防御黑客攻击最基本的要求。下面简单介绍一下黑客常用命令的使用方法。

### 1.5.1 ping命令

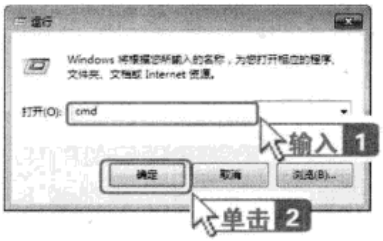
ping命令是黑客首先要掌握的命令，主要用来检查网络是否畅通和网络连接的速度，它所利用的原理是：网络上的计算机都有唯一确定的IP地址，用户给目标IP地址发送一个数据包，对方就要返回一个同样大小的数据包，根据返回的数据包可以确定目标主机的存在，初步判断目标主机的操作系统等信息。

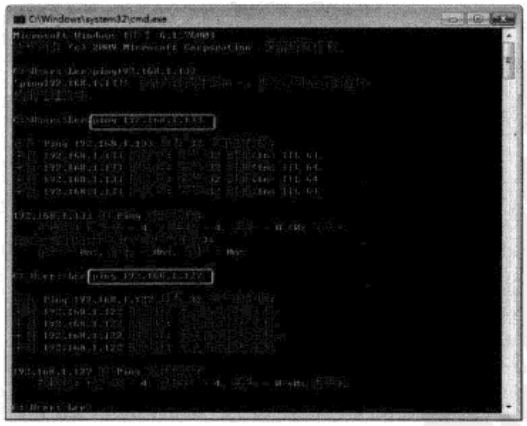
ping命令事实上是一个测试程序，如果ping命令运行正确，基本上可以排除物理层、数据链路层和网络层存在故障的可能性，从而大大减小出现问题的范围。按照Windows的默认设置，其ping命令发送4个ICMP（网间控制报文协议）回送请求，每个为32字节，如果一切正常，应该能得到4个回送应答。ping命令可以以毫秒为单位显示发送回送请求到返回回送应答之间的时间量，时间量越小，代表数据包通过的路由器越少或网速越快。

在Windows 7系统中利用ping命令测试网络连通状态的具体步骤如下。

步骤1 选择【开始】➢【运行】菜单项，在弹出的【运行】对话框中的【打开】下拉列表中输入“cmd”命令，然后单击 确定 按钮。

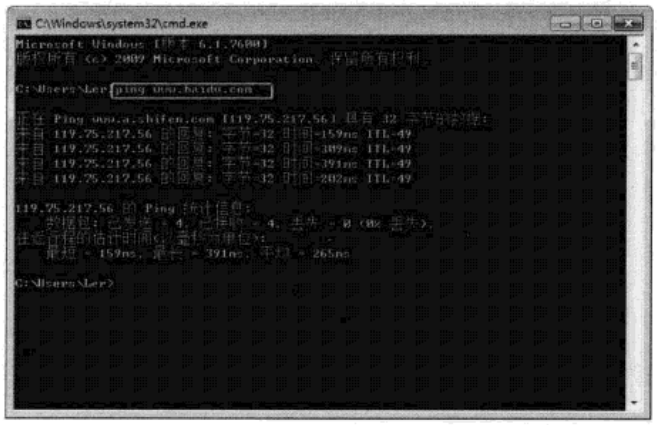
步骤2 在弹出的【命令提示符】窗口中输入ping命令，ping命令的格式为“ping+空格+IP地址”，这里ping是一个局域网的IP，即输入“ping 192.168.1.133”，然后按下【Enter】键。如果显示有字节的回复，就说明两台计算机之间是连通的；如果显示“无法访问目标主机”，说明两台计算机不能连通。



步骤3 此外，用户还可以使用“ping+空格+网站网址”的方法测试本机与网络上某个远程主机的

连通状态。例如，在【命令提示符】窗口中输入“ping www.baidu.com”，按下【Enter】键后可以看到网络是连通的。




下面介绍ping命令的几个常用参数。

-l size：发送size指定数据量的数据包。在默认的情况下，ping命令发送数据包的大小为32字节，使用-l size可以重新定义发送数据包的大小，但有一个大小的限制，就是最大只能发送65 500字节，这是因为Windows系列操作系统都有一个安全漏洞，就是当向对方一次发送的数据包不小于65 532字节时，对方就可能无法正常工作，微软公司为了解决这一安全漏洞，就限制了ping的数据包大小。

-f：在数据包中发送“不要分段”标志，数据包就不会被路由上的网关分段，通常所发送的数据包都会先通过路由分段再发送给目标主机，加上此参数后路由就不会再进行分段处理。

-i TTL：指定TTL值在目标主机的系统中停留的时间。

-v tos：将“服务类型”字段设置为tos指定的值。

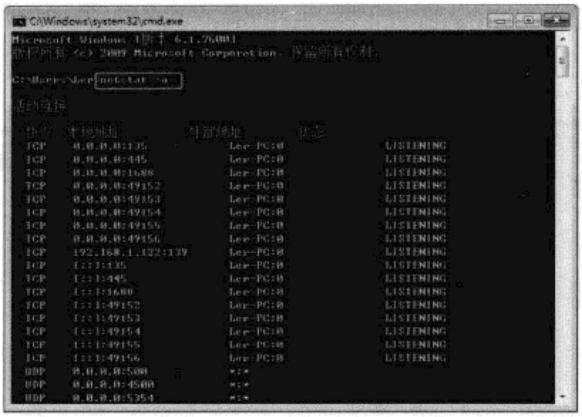
-r count：在“记录路由”字段中记录传出和返回数据包的路由。一般情况下，发送的数据包是通过一个个路由才到达目标地址的，但到底经过了哪些路由呢？通过此参数就可以设定想探测经过的路由的个数，不过限制只能跟踪到9个路由。

### 1.5.2 netstat命令

netstat命令用来查看网络状态，其操作简便，功能也很强大，主要用于显示与IP、TCP、UDP以及ICMP相关的统计数据，一般用于检验本机各端口的网络连接情况。该命令的格式如下。

netstat【-a】【-b】【-e】【-n】【-o】【-p proto】【-r】【-s】【-v】【interval】

-a：显示所有连接和监听的端口。




-b：显示包含于创建每个连接或监听端口的可执行组件。

-e：显示以太网统计信息。

-n：以数字形式显示地址和端口号。

-o：显示与每个连接相关的所属进程ID。

-p proto：显示proto指定的协议的连接。

-r：显示路由表。


-s：显示按协议统计。

-v：显示所有可执行组件。

Interval：重新显示选定的统计信息，每次显示之间有一个时间间隔（以秒计），按【Ctrl】+【C】组合键停止显示统计信息。如果省略，netstat则显示当前的配置信息。

### 1.5.3 net命令

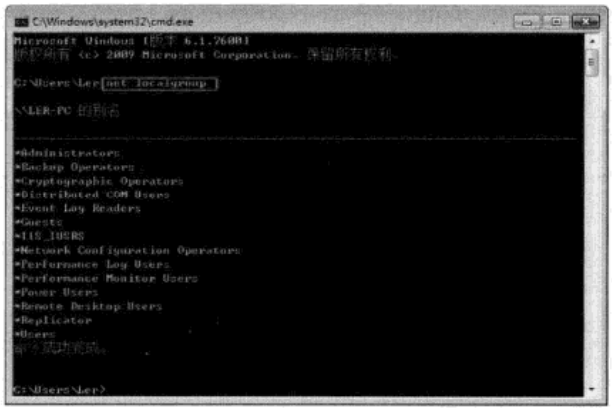
net命令是功能强大的以命令行方式执行的工具。它具有管理网络环境、服务、用户、登录等管理功能，内置于Windows系统中。下面介绍几种net命令的不同用法。

#### 1. net localgroup

该命令用于添加、显示或更改用户组。命令格式为net localgroup groupname{/add [/comment:text]|/delete}[/domain]。

其中，“groupname”是要添加、扩充或删除的本地组的名称；“/add”是将全局组名或用户名添加到本地组中；“comment：text”是为新建或现有组添加注释；“/delete”是从本地组中删除组名或用户名；“/domain”是在当前域的主域控制器中执行操作。

在【命令提示符】窗口中输入不带参数的“net localgroup”，显示服务器名称和计算机的本地组名称。




在介绍命令之前先创建一个用于实验的组，具体的操作步骤如下。

步骤1 选择【开始】➤【控制面板】菜单项，打开【控制面板】窗口，双击【管理工具】图标。

步骤2 弹出【管理工具】窗口，双击【计算机管理】图标。

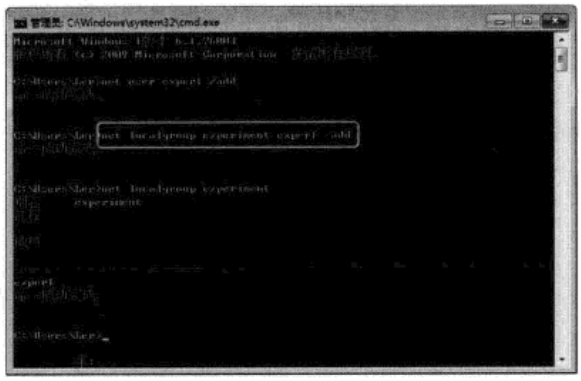
步骤3 弹出【计算机管理】窗口，在【本地用户和组】选项展开的列表中选择【组】选项，然后在该选项上单击鼠标右键，在弹出的快捷菜单中选择【新建组】菜单项。

步骤4 弹出【新建组】对话框，在【组名】文本框中输入“experiment”，单击 创建(C) 按钮，然后单击 关闭(O) 按钮即可完成创建。

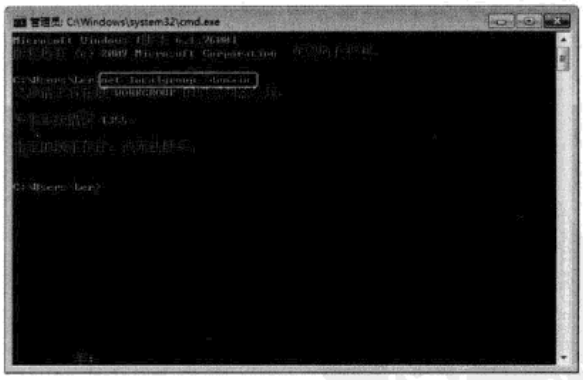

下面介绍该命令的常用参数。

/comment “text”：为新建或现有组添加注释。

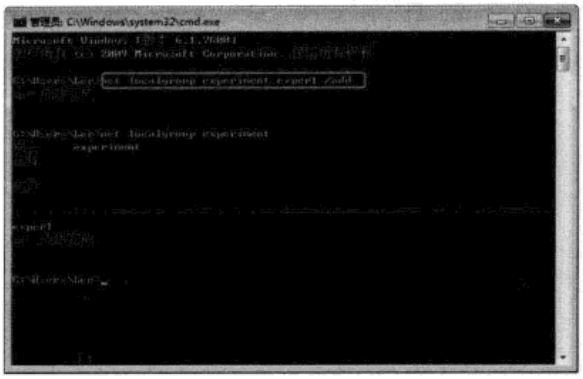
name：列出要添加到本地组或从本地组中删除的一个或多个用户名或组名。输入命令net localgroup experiment exper1 /add，就可以将用户“exper1”加入组“experiment”中（在运行该命令之前先用“net user exper1 /add”命令创建“exper1”用户）。



/domain：在当前域的主域控制器中进行操作，否则仅在本地计算机上进行操作。输入命令net localgroup /domain，如果没有域控制器，就会出现错误，错误号为1355。



/add：将全局组名或用户名添加到本地组中。



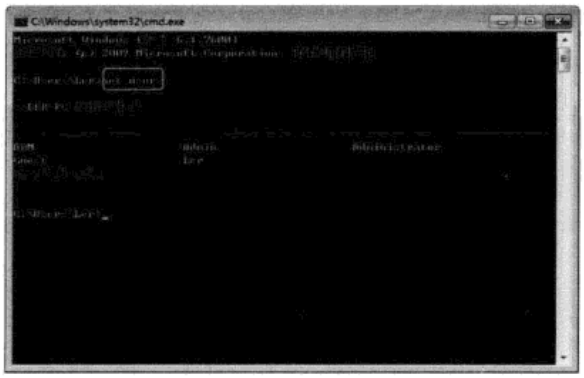
/delete：从本地组中删除组名或用户名。输入命令net localgroup experiment exper1 /delete，就可以将用户“exper1”从组“experiment”中删除。

## 2. net user

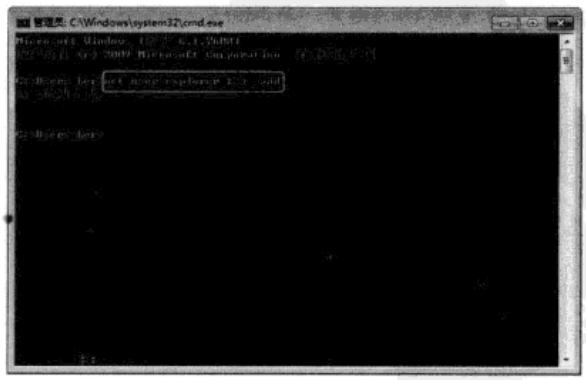
net user命令主要用来显示账户信息，修改、添加或删除账户。命令格式为net user[username[password|*]][/domain]或net user[username[password|*]]/add[options][/domain]或net user[username[/delete][/domain]]。

其中，username指定要添加、删除、修改或查看的用户账户名称，password为用户账户指定或更改密码。输入星号（*）将给出密码的提示，在密码提示符下输入密码时不显示密码。domain是指在域控制器上进行操作。

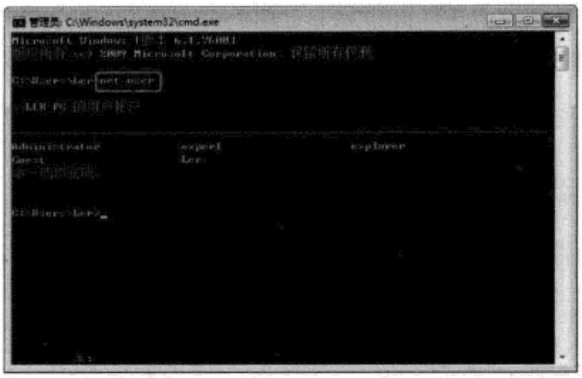
步骤1 输入不加参数的net user命令查看计算机上的用户账户列表。



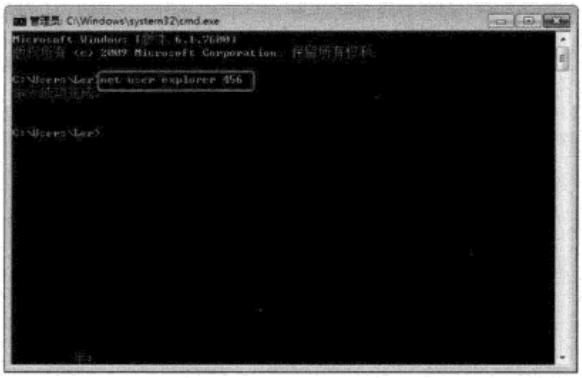
步骤2 建立一个用户名为“explorer”、密码为“123”的账户，命令为“net user explorer 123 /add”。



步骤3 用“net user”命令查看账户是否添加成功。

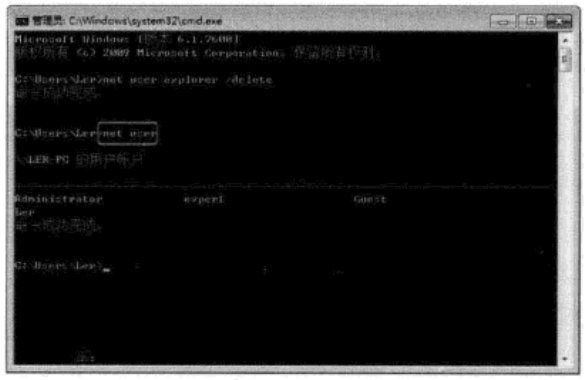


步骤4 对上面建立的用户的密码进行修改，由“123”改为“456”，命令为net user explorer 456。



步骤5 使用这个命令还可以将用户账户删除，例如，删除“explorer”账户的命令是net user explorer /delete。

步骤6 用“net user”命令查看，可以发现“explorer”账户已被删除。



## 1.5.4 DOS基本命令

DOS作为微软开发的第一款操作系统，虽然功能不是很强大，但由于其命令操作快捷，所以随着操作系统的发展保留了下来，且功能越来越强大。

DOS命令从文件和磁盘操作到网络和多媒体操作等都能方便地做到，而且能做许多在Windows等系统或环境下做不到或做不好的事。

下面介绍几个常用的DOS命令（DOS命令是不区分大小写的）。

### 1. DIR 命令

DIR命令用来显示文件和文件夹（目录），其命令格式为：DIR[文件名][参数]。它有很多参

数，如/A表示显示所有文件（包括隐藏属性和系统属性的文件），/S表示显示子文件夹中的文件，/P表示分屏显示，/B表示只显示文件名。

步骤1 用不带参数的命令浏览D盘下的文件，其命令为“DIR D:”。

步骤2 如果用户想查看隐藏文件和系统文件，就需要加上参数“/A”，命令为“DIR D: /A”。

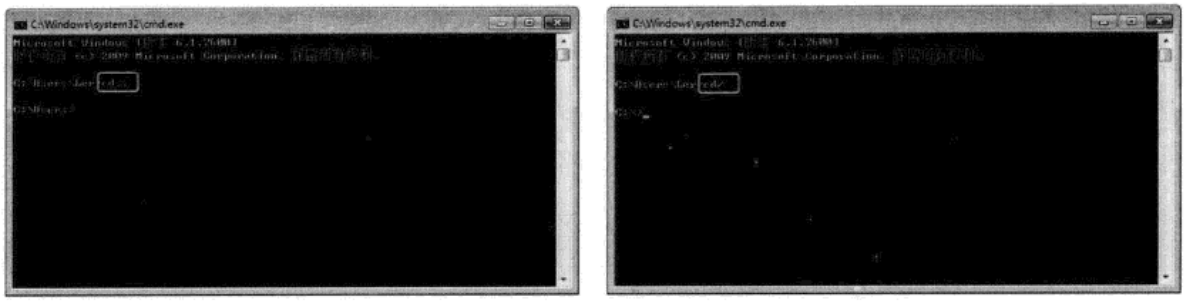
步骤3 如果只输入“DIR”，就表示查看当前路径下的文件。


## 2. CD 命令

CD（CHDIR）命令用来退出或进入文件夹，这个命令常和DIR命令一起使用。

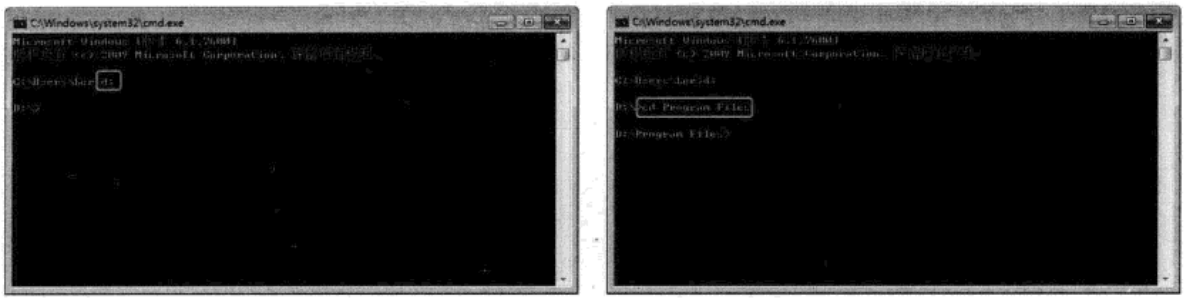
步骤1 当用户想要返回当前目录的上一级目录时，就需要输入“CD..”命令。

步骤2 如果用户想要直接回到当前目录的根目录，就需要输入“CD\”命令。



步骤3 直接输入“盘符:”后按下【Enter】键就可以改变盘符，例如，输入“d：”将盘符改到了D盘。

步骤4 CD命令更多的时候是用来进入一个文件夹，命令格式为：CD[文件夹名]。例如，输入“cd Program Files”可以进入D盘下的Program Files文件夹。



### 3. MD 和 RD 命令

MD命令用于新建一个文件夹，RD命令用于删除一个文件夹。新建一个文件夹的命令是MD[文件夹名]，同样，删除一个文件夹的命令是RD[文件夹名]。

步骤1 在D盘根目录下新建一个名为“exp”的文件夹，输入md exp。

步骤2 进入【（D：）】窗口，就会看到新建立的文件夹。

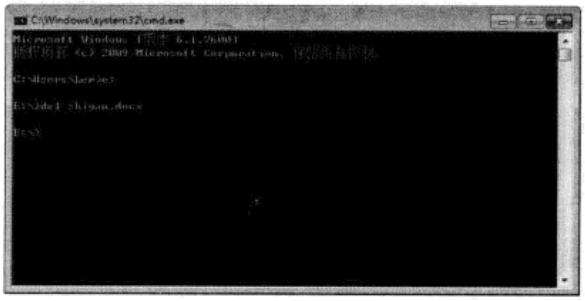
步骤3 用RD命令删除刚刚建立的文件夹（只能用来删除空文件夹），命令为RD exp。

步骤4 如果是非空文件夹，则要加参数/S。例如，删除D盘根目录下的非空文件new，输入“rd new /s”，当提示确认时输入“y”即可。

### 4. DEL 命令

该命令用于删除文件，格式为：DEL[文件名]。

例如，删除E盘目录下的shiyan.docx。

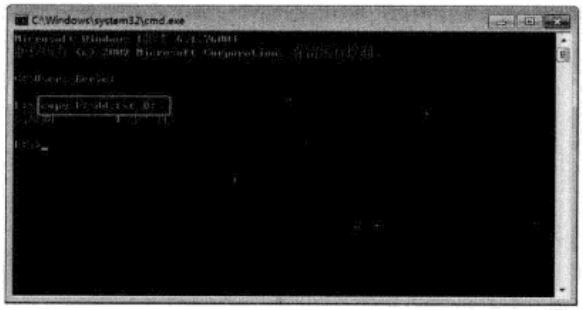


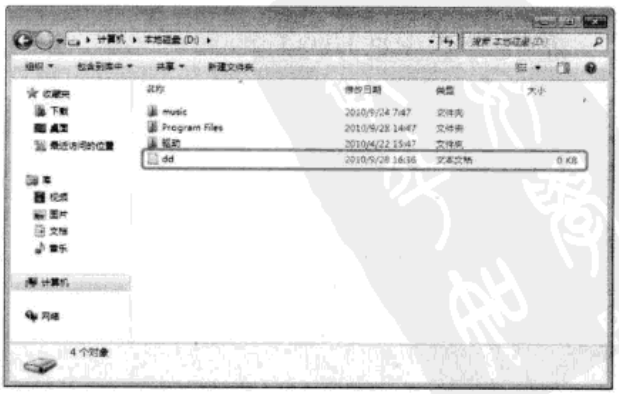
### 5. COPY 命令

该命令用来复制文件或合并文件。

复制文件的命令格式为：COPY[源路径名][源文件名][目标路径名]。

例如，将E盘下的dd.txt复制到D盘下，命令为COPY E:\dd.txt D:\。打开D盘就会发现dd.txt文件。





合并文件的命令格式为：COPY /B[文件1+文件2+…文件N][合并后的文件名]。

步骤1 将E盘下的1.txt、2.txt和3.txt合并为4.txt文件，命令为COPY /B 1.txt+2.txt+3.txt 4.txt。

步骤2 打开E盘会发现合并出了一个4.txt文件。

## 新手问题解答

### 如何用 DOS 命令向计算机系统中注入一个“.dll”文件

电脑在使用过程中，有时候会遇到“.dll”文件丢失的现象，在下载“.dll”文件后，需要将其添加到电脑系统盘中的system32文件夹中。

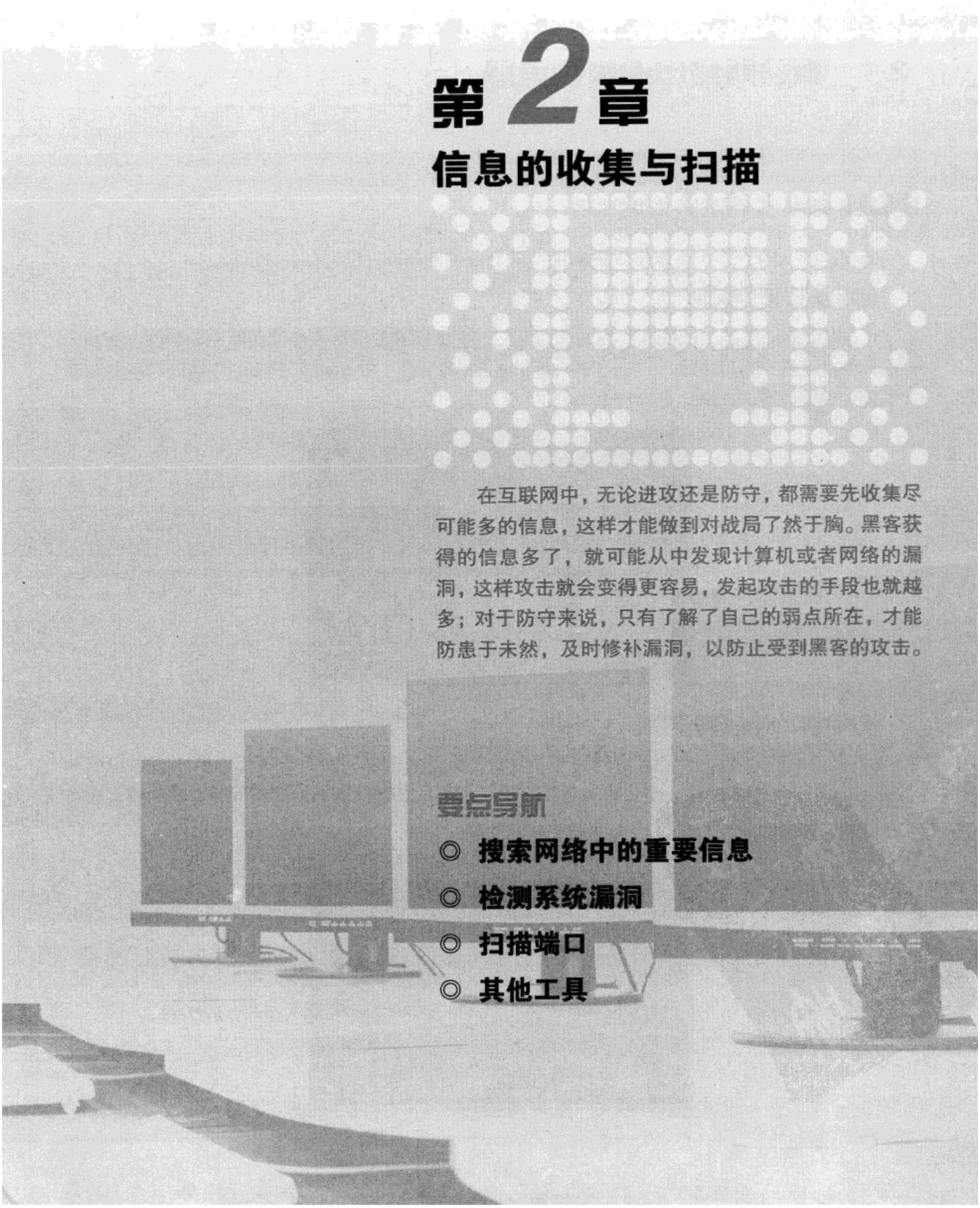
选择【开始】➢【运行】菜单项，在弹出的【运行】对话框的【打开】下拉列表中输入“cmd”，然后按下【Enter】键。

弹出【命令提示符】对话框，利用cd命令进入下载的“.dll”文件所在的文件夹中。

然后利用copy命令将其添加到系统盘下的system32文件夹中（一般添加到C:\Windows\system32目录下）。

### 如何检测与某个计算机的连通性

在【命令提示符】窗口中，输入“ping X”（X为该计算机的IP地址），然后按下【Enter】键即可。



# 第2章
# 信息的收集与扫描

在互联网中，无论进攻还是防守，都需要先收集尽可能多的信息，这样才能做到对战局了然于胸。黑客获得的信息多了，就可能从中发现计算机或者网络的漏洞，这样攻击就会变得更容易，发起攻击的手段也就越多；对于防守来说，只有了解了自己的弱点所在，才能防患于未然，及时修补漏洞，以防止受到黑客的攻击。

**要点导航**

- ◎ 搜索网络中的重要信息
- ◎ 检测系统漏洞
- ◎ 扫描端口
- ◎ 其他工具

## 2.1 搜索网络中的重要信息

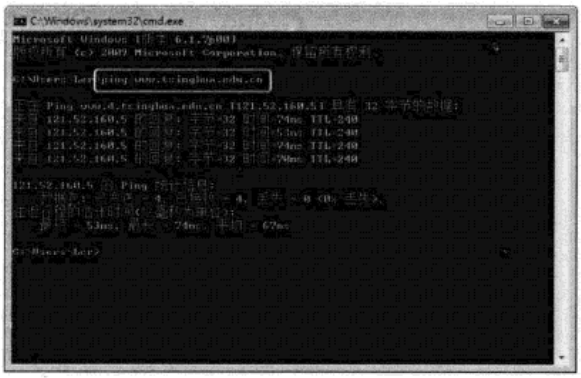
信息的收集和分析过程在黑客进行攻击的整个过程中往往是耗时最长的，这包括收集大量的目标信息，经过详细分析找出漏洞以及确定入侵方案等，而真正的入侵可能只需要很短的时间。

### 2.1.1 获取目标主机的IP地址

使用前面介绍过的一些常用黑客命令可以很容易地获取一些网站的IP地址。

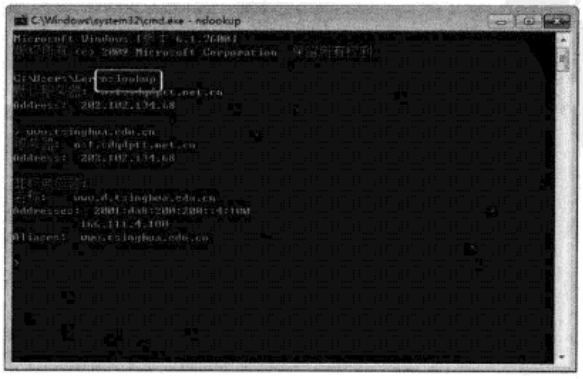
#### 1. 使用 ping 命令获取

可以使用ping命令来试探一些网站的IP地址，这里以获取清华大学的IP地址为例进行介绍，在【命令提示符】窗口中输入“ping www.tsinghua.edu.cn”，然后按下【Enter】键即可得到清华大学WWW服务器的IP地址是121.52.160.5。



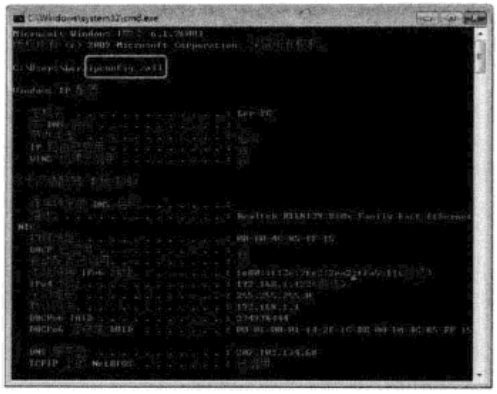

#### 2. 使用 nslookup 命令获取

nslookup命令也是一个经常使用的可以查询IP地址的命令。在【命令提示符】窗口中输入“nslookup”，按下【Enter】键后可以看到本机所用的DNS服务器，然后输入要查询的域名即可得到结果。Address后面列出的即为要查询的IP地址。



## 2.1.2 获取目标主机的物理地址

有时候需要查询目标主机的物理地址，那该如何获取呢？

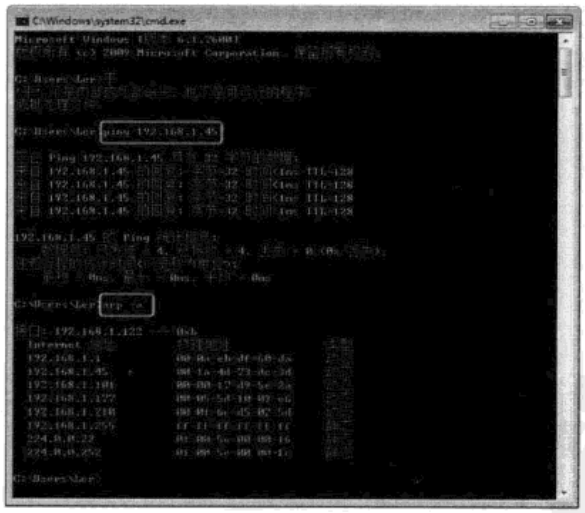


如果目标主机正常运行或者被授权进行操作，用户可以在【命令提示符】窗口中直接输入“ipconfig /all”命令进行查询。

另外，如果用户知道目标主机的IP地址，可以查找同一网段的目标主机的物理地址。下面以获取同一网段中IP地址为192.168.1.45的目标主机的物理地址为例进行介绍，具体的操作步骤如下。

步骤1 在【命令提示符】窗口中输入“ping 192.168.1.45”命令，然后按下【Enter】键便可看到本地主机和目标主机是连通的。

步骤2 输入“arp -a”命令，并按下【Enter】键，可以从下方的列表中查找到IP地址为“192.168.1.45”选项，接着从其对应选项中便可查看其物理地址为“00-1a-4d-73-dc-3d”。



## 2.1.3 了解网站备案信息

一个网站在正式发布之前，需要向有关机构备案申请域名，申请域名的信息称为网站备案信息，这些信息通常是公开的。

网站备案信息保存在域名管理机构的数据库里，因为大多数都是公开的，所以任何人都可以对其进行查询。这些公开的网站备案信息中会有许多敏感的信息，主要包括以下几个方面。

(1) 注册人的姓名。

(2) 注册人的E-mail，甚至联系电话、传真。

(3) 注册机构、通信地址、邮政编码。

(4) 注册有效时间、失效时间。

有许多网站可以查询网站备案信息，在中国比较权威的机构是中国互联网络信息中心（http://www.cnnic.com.cn），它记录了所有cn域名的注册信息。这里以“谷歌”为例介绍如何查询网络备案信息。具体的操作步骤如下。

步骤1 打开浏览器，在地址栏中输入“http://www.cnnic.cn”，按下【Enter】键，打开中国互联网络信息中心网站，在【WHOIS查询】下的【输入您想要查询的CN域名、中文域名、通用网址、IP地址、可信服务器证书】文本框中输入“google.cn”，并选中文本框下面的【CN域名】单选钮，然后单击 查 询 按钮。

步骤2 进入下一个查询界面，在【验证码】文本框中输入在【在验证码框输入】中看到的验证码，然后单击 查 询 按钮。


步骤3 稍等片刻即可看到所查询的域名的详细信息。

## 了解中国互联网信息中心（CNNIC）

中国互联网络信息中心（China Internet Network Information Center，CNNIC）是经国家主管部门批准，于1997年6月3日组建的管理和服务机构，行使国家互联网络信息中心的职责。

作为中国信息社会重要的基础设施建设者、运行者和管理者，中国互联网络信息中心（CNNIC）以“为我国互联网络用户提供服务，促进我国互联网络健康、有序发展”为宗旨，负责管理维护中国互联网地址系统，引领中国互联网地址行业发展，权威发布中国互联网统计信息，代表中国参与国际互联网社群。


## 2.2 检测系统漏洞

通过扫描，黑客可以找到别人的系统漏洞，从而确定攻击方案；系统管理员也可找到自己系统的漏洞并进行修补，从而提高安全系数。

### 2.2.1 什么是扫描器

扫描器作为黑客常用的一种工具软件，是一种自动检测远程或本地主机安全性弱点的程序。

#### 1. 扫描器的种类

通过使用扫描器，用户可以不留痕迹地发现远程服务器的各种TCP端口的分配、提供的服务以及它们的软件版本，这就可以了解远程主机所存在的安全问题。

扫描器的种类主要有以下3种。

(1) 网络扫描器：网络扫描器在网络上搜索以找到网络上的所有主机。

(2) 网络漏洞扫描器：网络漏洞扫描器将网络扫描器向前发展了一步，它能检测目标主机，并突出一切可以为黑客利用的漏洞。

(3) 主机漏洞扫描器：这类工具就像是一个有特权的用户，它从内部扫描主机，检测口令强度、安全策略以及文件许可等内容。

### 2. 扫描器的工作原理

扫描器采用模拟攻击的形式对目标可能存在的已知安全漏洞进行逐项检查，目标可以是工作站、服务器、交换机、数据库应用等各种对象。然后根据扫描结果向系统管理员提供周密可靠的安全性分析报告（包括能否用匿名登录，是否有可写的FTP目录，能否用TELNET，等等），为提高网络安全整体水平提供重要依据。

### 3. 扫描器的作用

扫描器是能帮助用户发现目标主机某些存在的弱点的工具。这些弱点可能是破坏目标主机安全的关键。对于一个刚入门的黑客来说，这些数据可能是毫无意义的，而对于一个掌握和精通各种网络应用程序漏洞知识的黑客来说，其价值可能远远超过几百个有用的账号。一个好的扫描器能对其得到的数据进行分析，帮助用户查找主机的漏洞，但它不会提供进入一个系统的详细步骤。

## 2.2.2 IPScan网段扫描工具

IPScan网段扫描工具能够帮助网络管理员有效地管理访问网络的IP/MAC资源，并且能够利用强大的切断功能来保障企业内部的安全。IPScan自动收集网上的全部IP/MAC相关信息，实时提供更新数据，在中央控制未经许可的IP/MAC地址访问网络，从而提高网络的安全性。IPScan能防止一般用户与路由器、服务器等重要设备发生IP冲突，保护重要设备的IP，保证网络稳定地运行。

IPScan工具的其他功能如下。

(1) 能帮助用户提高网络管理水平及网络安全等级。

(2) 在DHCP网络环境中提高网络安全。

(3) 能够检测和控制未知的或未经授权的用户。

(4) 防止与网络中重要设备的IP地址发生冲突。

(5) 防止用户擅自变更IP地址。

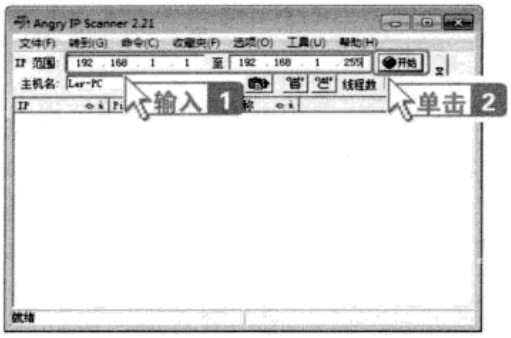
(6) 帮助网络管理员了解IP使用的每个细节。

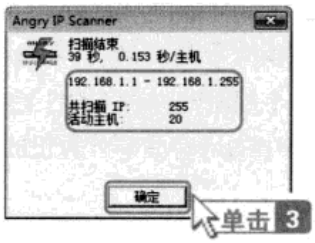
(7) 从一个中央位置控制整个网络的访问。

下面以Angry IP Scanner 2.2.1为例进行介绍。从网上下载该工具后就可以直接运行。具体的操作步骤如下。

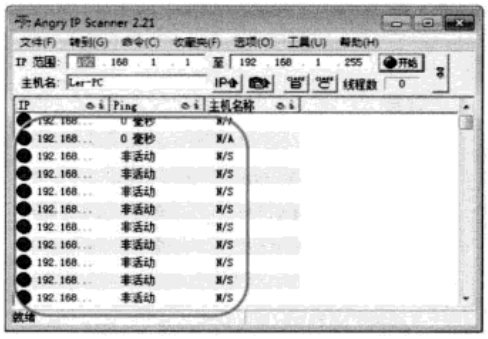
步骤1 打开IPScan，在【IP范围】文本框中输入起始IP和终止IP，然后单击 开始 按钮。

步骤2 扫描完毕后弹出一个提示对话框，显示在设定的IP地址段中共扫描了255个IP地址，其中有20个IP地址是活动的，然后单击 确定 按钮。




步骤3 随即在下方的列表框中列出比较详细的主机信息。




## 2.2.3 LanSee局域网查看工具

局域网查看工具（LanSee）主要用于对局域网上的各种信息进行查看。它采用多线程技术，搜索速度很快。它将局域网中比较实用的功能完美地融合在一起，如搜索计算机（包括计算机名、IP地址、MAC地址、所在工作组和用户）、搜索共享资源（包括HTTP和FTP服务）等。该工具具有搜索计算机、搜索共享资源、搜索共享文件、发送消息、高速端口扫描、嗅探服务、多线程复制文件等功能。它是一款绿色软件，解压后直接打开即可运行，无需安装。

其主要功能如下。

(1) 搜索指定网段中的计算机，并显示每台计算机的计算机名、IP地址、工作组、MAC地址、用户名以及该网段中的所有共享资源和共享文件等。

(2) 将指定共享资源映射成本地驱动器。

(3) 搜索选定的一个或几个共享资源内的共享文件。

(4) 在搜索共享文件时可以选择搜索一种或者几种文件类型的共享文件。

(5) 打开指定的计算机、共享目录和共享文件等。

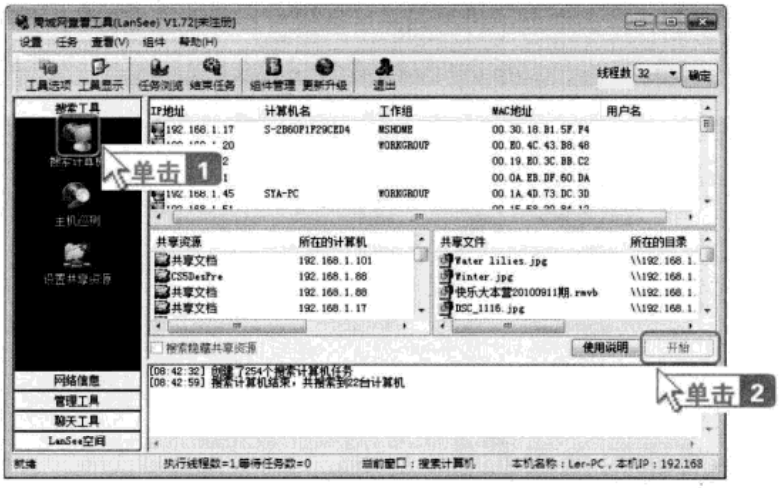
(6) 发送消息，既可以给选定的一台或几台计算机发送消息，也可以给指定工作组内的所有计算机发送消息。

(7) 扫描端口，既可以扫描出局域网内或指定网段内所有开放指定TCP端口的计算机，也可以扫描出指定计算机上所有活动的TCP端口。

(8) ping指定计算机，查看指定计算机的MAC地址、所在工作组以及当前用户等。

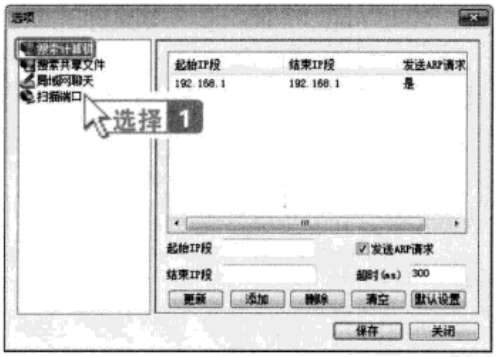
下面以局域网查看工具（LanSee）1.72为例进行介绍。

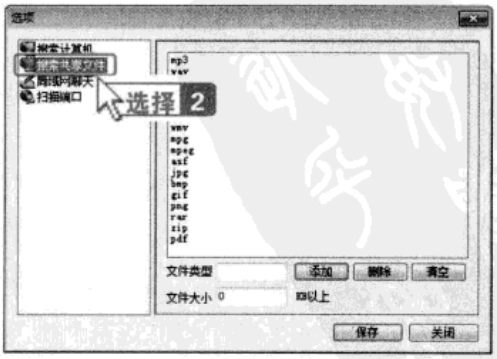
步骤1 打开【局域网查看工具】窗口，单击【搜索计算机】按钮，然后单击 开始 按钮，即可搜索局域网中的所有活动计算机的IP地址、计算机名、工作组、MAC地址、用户名、共享资源和共享文件等。




步骤2 如果想要设置搜索选项，可以通过单击 按钮来进行设置。单击 按钮，弹出【选项】对话框，在左侧的窗格中选择【搜索计算机】选项，可以在其右侧对计算机搜索进行设置。

步骤3 同样，在左侧的窗格中选择【搜索共享文件】选项，可以对要搜索的共享文件的类型和大小进行设置。



对共享文件搜索进行设置的方法相似，这里不再赘述。

局域网查看工具是一个非常实用的小工具，它的其他功能将在以后进行介绍。

### 2.2.4 LanExplorer全能搜索利器

LanExplorer采用类似资源管理器的界面，无需安装，操作方便，功能强大。作为一款优秀的搜索工具，与其他同类工具相比，它最大的优势是支持多线程搜索，用户可以利用该软件同时搜索局域网上所有的工作组、主机、打印机、共享文件，还可以自定义搜索文件。可以看出LanExplorer是局域网中的全能搜索利器。

LanExplorer占用的空间不大，不到1MB，但其功能非常强大，主要有以下几个方面。

(1) 方便快捷地搜索、浏览局域网资源。可以多线程搜索局域网上所有的工作组、主机、打印机和共享文件等。

(2) 可以按照网上邻居、工作组和IP地址段自动搜索所有共享的文件或自定义搜索的文件。

(3) 内置nbtstat，能快速查找某一IP网段内的所有主机，并根据IP地址得到对方主机的主机名、工作组名、用户名、MAC地址等，速度极快。能将扫描和搜索的结果保存为文本文件或Excel电子表格文件。

(4) 能对某一地址范围的主机进行ping端口扫描操作，找出所有的Web服务器、FTP服务器等。能向某一主机发送消息。

(5) 在局域网主机间拷贝文件时，能提供文件和目录的断点续传的功能。

(6) 采用类似资源管理器的界面，操作十分方便。是绿色软件，开放源代码。

用户可以到网上下载LanExplorer。下面以LanExplorer 1.67为例进行介绍，下载解压缩LanExplorer 1.67后，双击程序图标运行该程序。

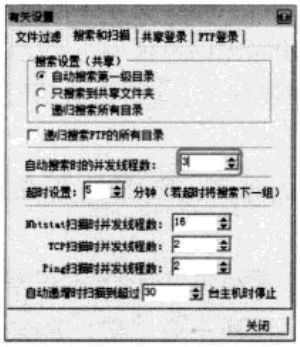
一般来说，默认的搜索设置并不方便用户进行搜索，这就需要进行设置。具体的操作步骤如下。

步骤1 单击工具栏中的 搜索设置 按钮，弹出【有关设置】对话框，从中可以设置资源的相关参数。

步骤2 例如，在【文件过滤】选项卡中的【要查找的文件名中包含如下文字：】文本框中输入“.doc”，然后单击 添加 按钮，将其添加到下面的【要查找的文件】列表框中，这样就可以搜索局域网中所有的.doc文件了。用户还可以设置使程序自动搜索所有共享的MP3、电影等各种类型的文件。

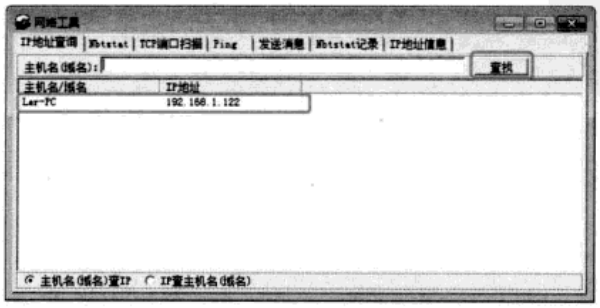


步骤3 还可以使用自动搜索功能进行搜索。切换到【自动搜索】选项卡，从中可以设置自动搜索的线程数，最大为10，还可以设置程序进行自动搜索的目录级别。




步骤4 设置完成后，单击 关闭 按钮，关闭【有关设置】对话框，然后单击想要搜索的工作组、主机或文件夹，即可进行自动搜索。

除了支持文件查询外，LanExplorer还支持IP地址查询以及计算机名查询。单击工具栏中的 IP地址查询 按钮，打开【网络工具】窗口，从中可以通过计算机主机名来查询IP地址，也可以通过IP地址来查询计算机主机名。例如，在【IP地址查询】选项卡的【主机名】文本框中输入计算机的名称，选中【主机名（域名）查IP】单选钮，然后单击 查找 按钮，就可以在列表中显示出对应计算机的IP地址。



单击窗口中的 IP地址段 按钮切换到IP地址搜索界面，在【起始】文本框和【终止】文本框中设置网段范围，然后单击 扫描 按钮，可以对该网段内所有活动计算机的信息进行扫描。此时也会弹出【网络工具】窗口，在该窗口的【Nbtstat】选项卡中可以根据IP地址得到所有活动主机的主机名、工作组名、用户名、MAC地址等信息。


另外，LanExplorer还提供了强大的鼠标右键功能。

## 2.2.5 MBSA微软基准安全分析器

Windows操作系统是用户最常用的电脑操作系统，但其安全性不够高，系统有很多漏洞，微软也不断地推出补丁。但由于操作系统漏洞的不确定性和数量的巨大，很少有人能了解Windows XP是否完全打上了所有的补丁，因此微软推出了一款名为Microsoft Baseline Security Analyzer（MBSA）的软件，用于操作系统的用户了解和修补系统的漏洞。

MBSA（微软基准安全分析器）Version 2.2包括可执行本地或远程Windows系统扫描的图形和命令行界面。MBSA V2.2可运行在Windows 2000、Windows XP、Windows Vista和Windows 7系统上，并且可以扫描Windows 2000以上版本的操作系统和IIS、SQL Sever、Internet Explorer和Office等，以发现常见的系统配置错误和缺少的安全更新。

用户可以在IE的地址栏中输入“http://www.microsoft.com/downloads/en/details.aspx?FamilyID=02be8aee-a3b6-4d94-b1c9-4b1989e0900c”，在微软的官方网站上下载MBSA2.2的安装程序。

### 1. MBSA 的功能

MBSA可以扫描本机或多台电脑、整个局域网的安全设置和系统漏洞，其主要功能有以下几个方面。

(1) 检查Windows操作系统的保密设置，包括是否安装修补程序（HOTFIXES）、是否启动

账号登录和退出检查、是否开启了Guset用户的账号、是否启动了没有必要启动而非常危险的网络服务，等等。

(2) 检查IIS的安全设置，其中包括是否安装了IIS LOCKDOWN TOOL、是否安装了IIS的安全补丁程序。

(3) 检查SQL Sever的安全设置内容。

(4) 检查Internet Explorer的设置。

(5) 检查OE/OUTLOOK的安全设置。

(6) 检查Microsoft Office的MACRO的安全设置。

在使用MBSA对系统进行检测之前需要确定以下几个必要条件。

(1) 如果计算机运行的是Windows XP以上版本的系统并且使用简单的文件共享，那么只能在本地进行检查。此时可以打开【控制面板】窗口，双击【文件夹选项】图标，打开【文件夹选项】对话框，然后切换到【查看】选项卡，取消选中【使用共享向导（推荐）】复选框。

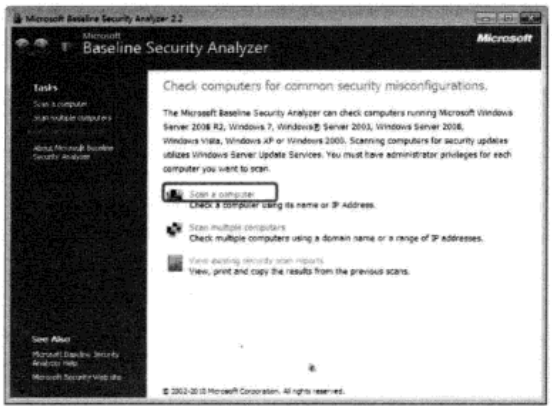

(2) 要检测局域网内其他计算机的安全性，必须有相应的网络管理权限。

## 2. 扫描单台计算机

MBSA在检测系统漏洞方面的功能是非常强大的，一般而言，单台计算机模式最典型的情况是“自扫描”，也就是扫描本地计算机。下面介绍如何使用MBSA检测单台计算机的Windows系统是否安全，具体的操作步骤如下。

步骤1 启动MBSA程序，打开其主界面，单击主界面右侧列表框中的【Scan a computer】选项。

步骤2 弹出【Which computer do you want to scan?】对话框，要想让MBSA能够成功地扫描计算机，就需要在此对话框中对参数进行设置。



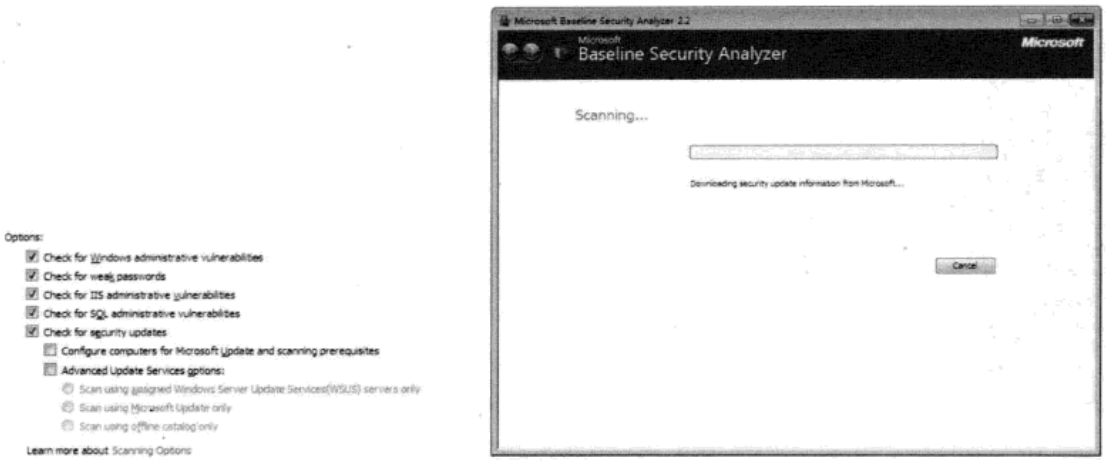


**步骤3** 设定要扫描的对象。MBSA提供了两种设置的方法：一种是在【Computer name】文本框中输入计算机的名称，格式为“工作组名\计算机名”。默认情况下MBSA会显示运行MBSA的计算机的名称，例如，图中的“WORK GROUP”是运行MBSA的计算机所属的工作组名称，“*error*”是计算机名称；另一种是在【IP address】文本框中输入计算机的IP地址。在文本框中允许输入同一网段中的任意IP地址，但不能输入跨网段的IP地址，否则会提示“Computer not found”（计算机没有找到）的信息。

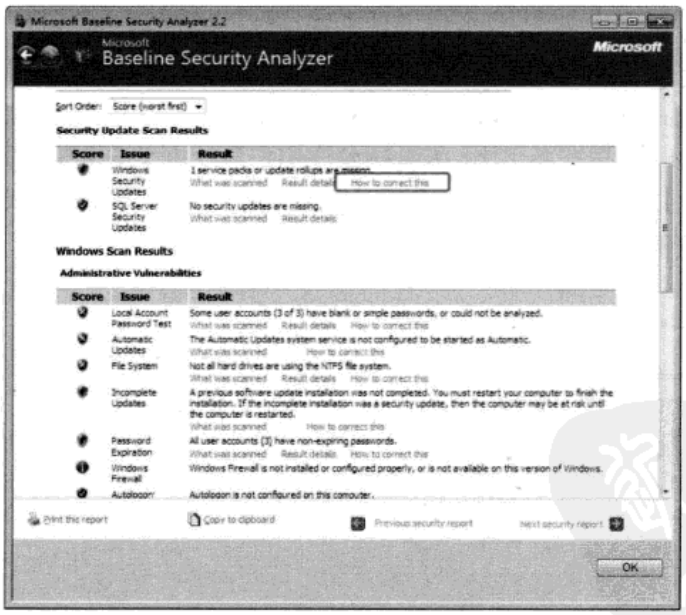
**步骤4** 设置安全报告的文件名格式。每次扫描成功后，MBSA会将扫描结果以“安全报告”的形式自动保存在“X:\Documents and Settings\;username\SecurityScans”（X是指Windows的系统分区符，username是指操作MBSA的用户名）下。MBSA允许用户自行定义安全报告的文件名格式，只要在【Security report name】文本框中输入文件名格式即可。MBSA提供了默认格式：“%D%-%C%(%T%)”（域名-IP地址（时间戳））。


**步骤5** 设定扫描中需要检测的项目，可以取消选中不必要的项目复选框以加快扫描速度。

**步骤6** 设置完成后，单击 Start Scan 按钮，弹出【Scanning...】对话框，MBSA开始对指定的计算机进行扫描。




步骤7 扫描完成会自动生成安全报告，用户可以根据安全报告【Score】列中不同颜色的图标来简单区分被扫描的计算机上哪些方面存在漏洞，哪些地方需要改进。如果检测项目的【Result】列中含有【How to correct this】选项，就应该单击该选项，然后根据解决方法下载相应的补丁程序或修改相关的设置，以修正存在的问题。

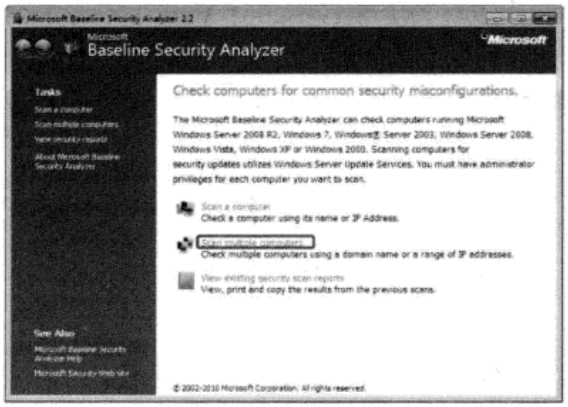


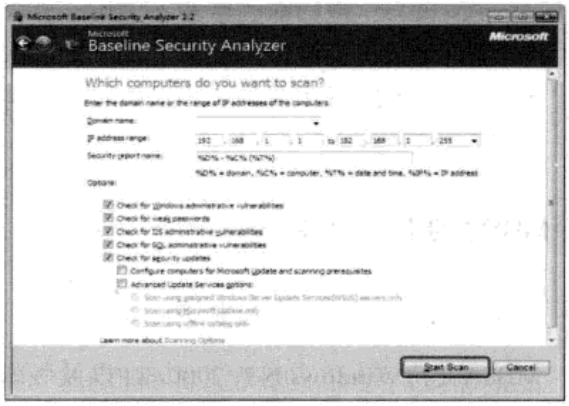

### 3. 扫描多台计算机

扫描多台计算机功能是扫描单台计算机功能的延伸，它只是将扫描对象扩大到网络中的一个域或IP地址段。它的工作原理与扫描单台计算机相同，即以安全漏洞为蓝本，对指定的域（或IP地址段）中的所有计算机进行逐一扫描。

步骤1 启动MBSA程序，打开其主界面，然后单击主界面中的【Scan multiple computers】（或者主界面左侧列表框中的【Scanmultiple computers】）选项。

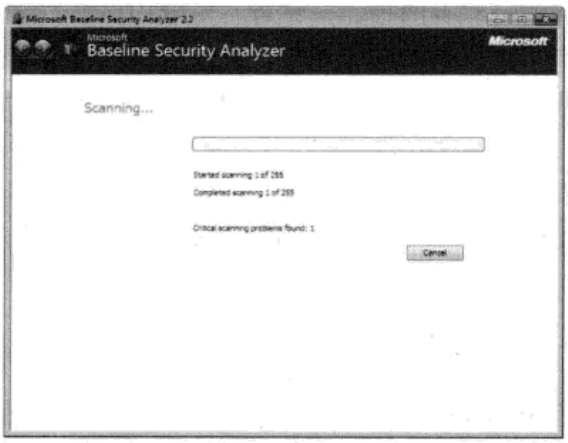
步骤2 弹出【Which computers do you want to scan?】窗口，在此窗口中也要进行必要的、准确的设置。此处的设置与扫描单台计算机时的设置相似，不同的是应在【Domain name】文本框中输入要扫描的域的名称，或者在【IP address range】文本框中输入要扫描的IP地址范围。设置完成后单击 Start Scan 按钮。

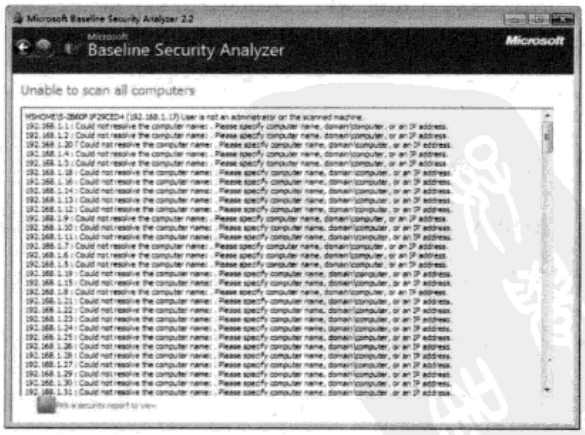



步骤3 弹出【Scanning...】对话框，MBSA开始依次扫描域或IP地址段中的每台计算机。完成扫描所需的时间与被扫描的计算机的数量和设置的扫描项目有关，一般来说，多台计算机的扫描会耗费比较多的时间。

步骤4 如果扫描成功，则会弹出安全报告窗口。但是，由于是扫描多台电脑，或者是网络或其他计算机的原因，可能会扫描失败，如果扫描失败，则会弹出窗口显示失败的原因。



### 扫描失败的原因主要有以下两种

(1) User is not an administrator on the scanned machine：被扫描的计算机上的用户不是系统管理员，出现这种情况的原因是用户没有以“Administrator”用户登录操作MBSA的计算机，或被扫描的计算机设置了登录密码。

(2) This is not a Windows NT/2000/XP/2003 Server or Workstation/Vista/2008 Server or Workstation：被扫描的系统不是Windows NT 4.0/2000/XP/Server 2003/Vista/Server 2008。出现这种情况的原因可能是使用了Windows 9X/Me系统或安装了非Windows操作系统，如Linux和UNIX操作系统。另外被扫描的对象根本不是计算机（如路由器等其他网络）也会出现这种情况。

## 4. MBSA 使用注意事项

### 不支持 Windows 9X 系统

MBSA支持Windows NT/2000/XP以及版本更高的系统，不支持Windows 9X系统。

### 不能分辨 Server 种类

MBSA不能分辨Windows Server所担当的角色，在一台普通的Windows Server电脑上同样可以发现一些只能在域控制器上才能发生的问题，用户使用时需要注意。

### 关于软件扫描

MBSA对Windows、Office、IIS等软件进行扫描的方式有两种，一种是“安全扫描”，这是指扫描以上软件是否进行了安全的配置，例如，IIS锁定工具是否已运行，文件系统是否都采用了NTFS格式等；另一种是“更新扫描”，是指扫描以上软件是否安装了最新的补丁程序。

### IE 限制

MBSA是基于IE页面开发的，因此MBSA需要在Internet Explorer 5.01以上才能运行，而且IE的所有设置项都会影响MBSA的运行。

### 需要手动进行修复

MBSA执行的是“基准扫描”，即只扫描和报告Windows Update定义的“关键更新”，而非所有更新。MBSA只扫描，不修补，需要用户手动进行修补。另外，按照MBSA的安全报告里的【How to correct this】选项进行修补并不能解决所有的问题，管理员需要按照MBSA的安全报告

逐个修补漏洞。

### 注意保护安全报告

每一次扫描后生成的安全报告都是以明码的形式保存在固定的文件夹中的，因此很容易被黑客利用从而找到计算机的漏洞数据。所以对安全报告应该另行处理（如打印、备份到其他目录等），然后彻底删除【SecurityScans】文件夹中的所有文件，以防被他人利用。

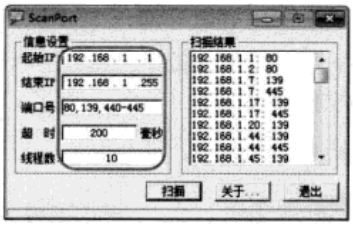
## 2.3 扫描端口

一个端口就是一个潜在的通信通道，也是一个入侵通道，对目标计算机进行端口扫描，会得到很多有用的信息。

### 2.3.1 ScanPort扫描端口利器

ScanPort（扫描端口利器）是一个小巧的网络端口扫描工具，也是一款绿色软件。

运行ScanPort工具，打开其主界面，在左侧的【信息设置】组合框的【起始IP】、【结束IP】、【端口号】、【超时】和【线程数】文本框中分别输入需要扫描的起始IP和结束IP、端口号、超时以及线程数，然后单击 扫描 按钮，随即在右侧的【扫描结果】列表框中列出扫描的结果。




### 2.3.2 SuperScan超级扫描器

对于网络管理员或者网络攻击者而言，一款好的扫描软件是必不可少的。一款好的扫描软件应该具备以下2个功能：一是功能强大。这里指的功能强大不是指功能很多，而是指软件提供的功能都可以取得很好的效果。二是应尽量在同一个领域做到全面。例如，扫描系统漏洞的软件最好兼顾该系统的所有版本和大部分的常见漏洞。下面介绍一款优秀的IP和端口扫描软件——SuperScan。

SuperScan不仅仅是一个端口扫描软件，它除了最重要的端口扫描功能之外，还有很多其他的功能。

(1) 通过ping命令来检验IP是否在线。

(2) IP和域名相互转换。

(3) 检验目标计算机提供的服务类别。

(4) 检验一定范围内的目标计算机是否在线和端口情况。

(5) 工具自定义列表检验目标计算机是否在线和端口情况。

(6) 自定义要检验的端口，并可以保存为端口列表文件。

(7) 自带一个木马端口列表trojans.lst，通过这个列表可以检测目标计算机中是否有木马，同时也可以自定义修改这个木马端口列表。

这款软件几乎具备了与IP扫描有关的所有功能，而且每个功能都很专业。使用SuperScan可以随意地选择端口，而且端口都有简单的说明，地址输入更轻松，在找到的主机上单击鼠标右键可以打开http浏览、telnet登录、ftp上传，以及nslookup域名查询等功能。

SuperScan 3.00的界面比较复杂，下面根据它的共享功能来介绍其使用方法。

### 1. 域名（主机名）和 IP 相互转换

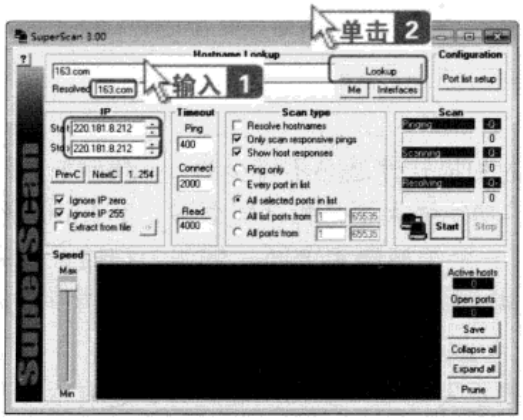
该功能用于取得域名对应的IP地址，如163.com的IP地址，或者根据IP地址来查找相应的域名，例如，根据202.106.185.77来取得域名。在SuperScan中有两种方法可以实现该功能。

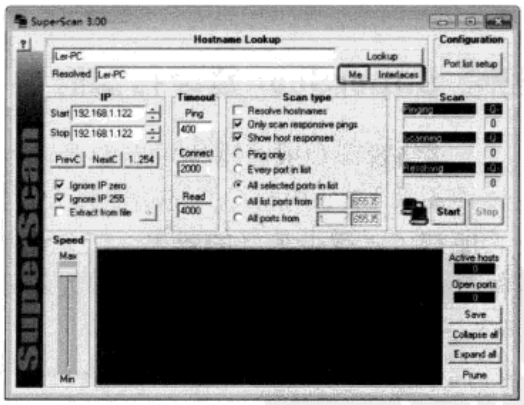
#### 通过 Hostname Lookup

第一种方法是通过Hostname Lookup来实现。具体的操作步骤如下。

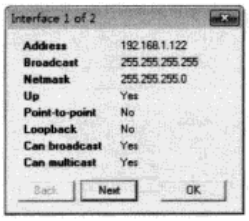
步骤1 启动SuperScan 3.00程序，打开其主界面，在【Hostname Lookup】组合框的【Resolved】文本框中输入要查询的域名（如163.com），单击 Lookup 按钮，在【IP】组合框中的【Start】微调框和【Stop】微调框中就会显示其IP地址。

步骤2 还可以单击 Me 按钮获取本机的IP地址。




步骤3 单击 Interfaces 按钮可以查看本地IP的设置情况。

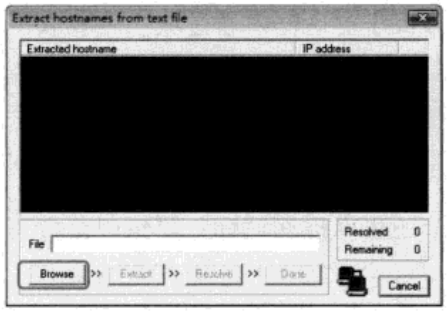


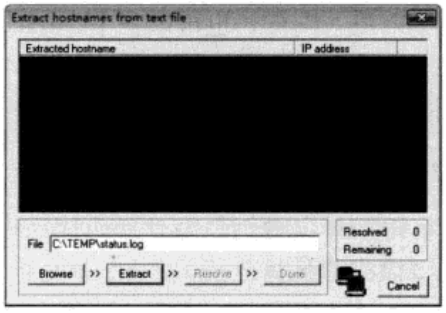

### 通过 Extract From File

第二种方法是通过Extract From File来实现的，该方法通过一个域名列表来将域名转换为相应的IP地址。

步骤1 选中【Extract from file】复选框，单击 → 按钮，打开【Extract hostnames from text file】对话框，然后单击 Browse 按钮。

步骤2 打开【Scan text file for IPs】对话框，在对话框中选中域名列表后单击【Extract hostnames from text file】对话框中的 Extract 按钮进行转换。

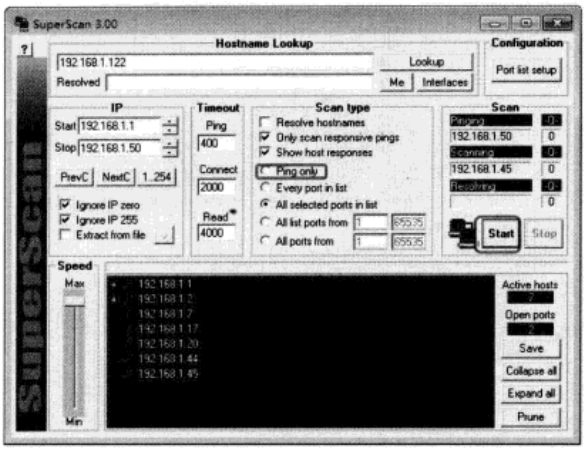



## 2. IP 功能的使用

ping主要用于检测目标计算机是否在线和通过反应时间判断网络状况。

在【IP】组合框中的【Start】微调框中输入起始IP，在【Stop】文本框中输入终止IP，然后选中【Scan Type】组合框中的【Ping only】单选钮，即可对该IP段内的当前正在活动的计算机进行ping操作。例如，要ping在162.168.1.1~192.168.1.50这一IP段内的计算机，在输入IP范围以及选中【Ping only】单选钮之后，单击【Scan】组合框中的 Start 按钮进行ping操作，在下方的列表框中列出的左侧打勾的IP地址即为当前正在活动的计算机的IP地址。




在以上设置中，用户可以使用以下复选框和按钮来快速设置：选中【lgnore IP zreo】复选框可以屏蔽所有的以0结尾的IP，选中【Ignore IP 255】复选框可以屏蔽所有以255结尾的IP，单击 PrevC 按钮可以直接转到前一个C网段，单击 NextC 按钮可以直接转到后一个C网段，单击 1..254 按钮可以直接选择整个网段。同样，也可以在【Extract From File】对话框中通过域名列表取得IP列表。在ping的时候，可以根据网络情况在【Speed】中设置相应的反应时间，一般采用默认值即可。因为SuperScan的速度非常快，结果也很准确，一般没有必要改变反应时间的设置。

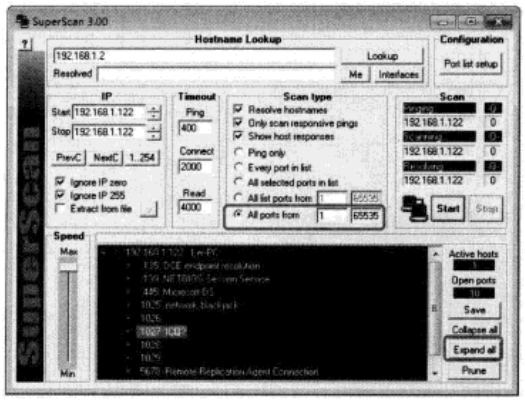
### 3. 端口检测

进行端口检测可以查询目标计算机提供的服务，还可以检测目标计算机中是否有木马。下面介绍进行端口检测的具体方法。

#### 检测目标计算机的所有端口

如果检测时没有特定的目的，只是为了了解目标计算机的一些情况，可以对目标计算机的所有端口进行检测。但一般不提倡进行这种检测，因为首先程序会对目标计算机的正常运行造成一定的影响，同时也会引起目标计算机的警觉；其次，该操作的扫描时间很长；再次，该操作浪费带宽资源，对网络的正常运行会造成一定的影响。

在【IP】组合框的【Start】微调框和【Stop】微调框中分别输入起始IP和终止IP，在【Scan Type】组合框中选中最下面的【All Ports From】单选钮并保持右侧文本框中的数值“1”和“65535”不变（如果需要返回计算机的主机名，可以选中【Resolve hostnames】复选框）。




这里是对IP地址为192.168.1.122的计算机的所有端口进行扫描的结果。扫描完成后单击 Expand all 按钮将扫描结果展开，可以看到这台计算机的详细信息：第一行是目标计算机的IP和主机名，从第二行开始的小圆点是所有扫描计算机的活动端口和对端口的解释。在右侧的【Active hosts】文本框中显示的是扫描到的活动主机数量，因为现在仅扫描了192.168.1.122这一台计算机，因此数量为“1”；在【Open ports】文本框中显示的是目标计算机打开的端口数，这里共扫描到了10个端口。

## 扫描目标计算机的特定端口

用户可以通过自定义端口的方式来扫描目标计算机的特定端口。

使用自定义端口有以下几个优点。

(1) 选择端口时可以详细了解端口的信息。

(2) 选择的端口可以自行命名保存，这样有利于再次使用。

(3) 可以根据特定的要求有的放矢地检测目的端口，节省时间和资源。

(4) 根据一些特定的端口，用户可以检测目标计算机是否被攻击者利用、种植了木马或是打开了不应该打开的服务。

下面介绍扫描目标计算机特定端口的具体步骤。

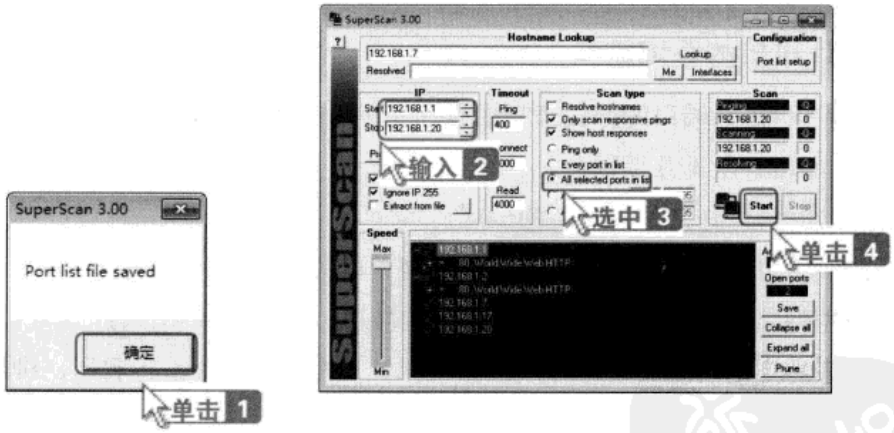
步骤1 单击主界面右上角的【Configuration】组合框中的 Port list setup 按钮打开【Edit Port List】对话框。在【Select ports】组合框中的列表框中双击需要扫描的端口，端口的前面即会出现一个“√”，例如，选择21（FTP服务）、23（Telnet服务）、80（Web服务）等3个端口。选择时要注意左边的【Change/Add/Delete port info】和【Helper apps in right-click menu】组合框，这两个组合框中包含关于此端口的详细说明和所使用的程序。当双击选中某个端口时，【Change/Add/Delete port info】组合框中的【Selected】复选框同时被选中。

步骤2 单击 Save 按钮打开【Save port list file】对话框，在【文件名】下拉列表中输入一个名称

作为列表的名称。设置完成后单击 保存(S) 按钮。


步骤3 弹出一个提示对话框，提示用户保存成功，接着单击 确定 按钮，返回【Edit Port List】对话框，然后单击 OK 按钮。

步骤4 返回主界面中，在【IP】组合框中的【Stat】微调框和【Stop】微调框中分别输入起始IP和终止IP，在【Scan Type】组合框中选中【All selected ports in list】单选钮，然后单击 Start 按钮开始检测。




## 2.3.3 在线端口扫描

扫描端口的方法很多，可以是手动扫描，也可以用端口扫描工具进行扫描，还有一种是在线端口扫描。下面介绍两种方便实用的在线端口扫描工具。

### 中国人在线端口扫描

“中国人在线端口扫描”（http://zhongguoren.cn/saomiao/）是一款非常方便快捷的在线端口扫描工具。下面具体介绍使用该扫描工具的方法。

步骤1 打开Internet Explorer 7.0浏览器，在地址栏中输入“http://zhongguoren.cn/saomiao/”，然后按下【Enter】键，打开【中国人在线端口扫描】页面，接着在【IP/域名】文本框中输入需要进行端口查询的IP地址或域名，在这里输入“163.com”，并在其下方选中【常用端口】单选钮，然后单击 查询 按钮。

步骤2 稍片刻，该扫描工具会将【IP/域名】文本框中的“163.com“自动转换为对应的IP地址，并在其下方以列表的形式列出该IP地址的各个端口的情况。

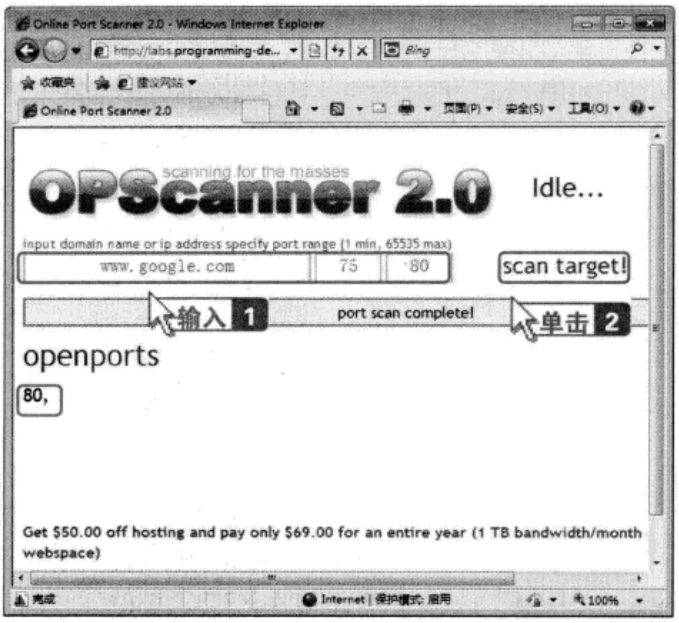


另外，用户还可以在【IP/域名】文本框中输入IP地址或域名后，选中【定义端口】单选钮，自定义端口。

## OPScanner

OPScanner（http://labs.programming-designs.com/portscanner/）可扫描1~665 535范围内的所有端口，如果某端口是开放的，就会在下方的openports栏中显示出来。虽然运行速度比较慢，但非常实用。

具体的操作方法是：在IE浏览器的地址栏中输入“http://labs.programming-designs.com/portscanner/”，并按下【Enter】键打开【OPScanner 2.0】页面，接着在“Input domain name or ip address specify port range（1 min，65535 max）下方的3个文本框中分别输入IP地址或域名、需要扫描的最小端口号和最大端口号，然后单击“scan target!”链接，该扫描工具便进行端口扫描，扫描完成后端口的情况列在下方的openports栏中。




## 2.4 其他工具

黑客对目标主机进行攻击时，首先需要进行扫描和探测，然后才能执行其他的任务。下面介绍一些黑客的常用于对目标进行扫描和探测的工具。

### 2.4.1 SSS扫描之王

黑客在入侵用户计算机之前首先要对其进行扫描，只有扫描出计算机中的安全漏洞，才能顺利地入侵。SSS就是一款非常专业的安全漏洞扫描软件，它能够扫描出计算机中存在的各种漏洞。

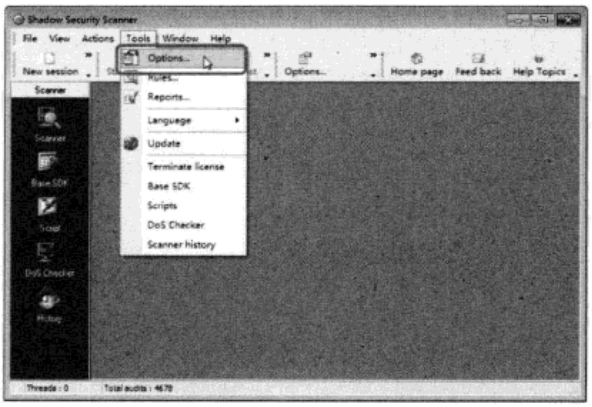
SSS扫描软件可以对很大范围内的系统漏洞进行可靠、安全、高效的检测，如果发现系统中存在被攻击的漏洞会给出相应的解决方法，因此了解这款软件的使用是非常有必要的。下面先介绍如何设置SSS扫描器的各功能选项。

SSS最重要的功能主要通过【Options】和【Rules】选项实现。

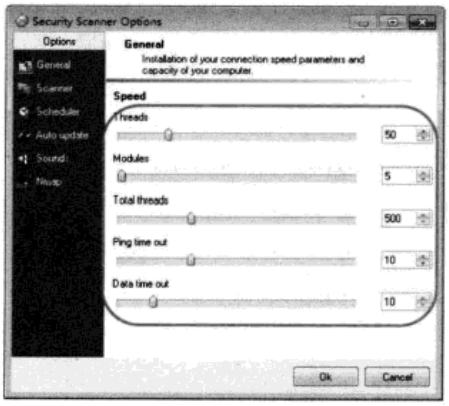
1. 【Options】选项

首先要将该软件下载并安装到计算机中（具体操作这里不再详细介绍），然后运行SSS程序。

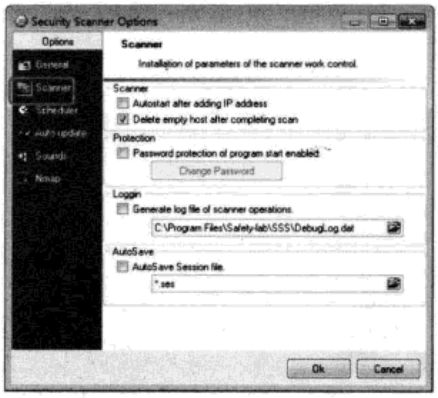
步骤1 打开SSS主窗口，然后选择【Tools】➢【Options】菜单项。



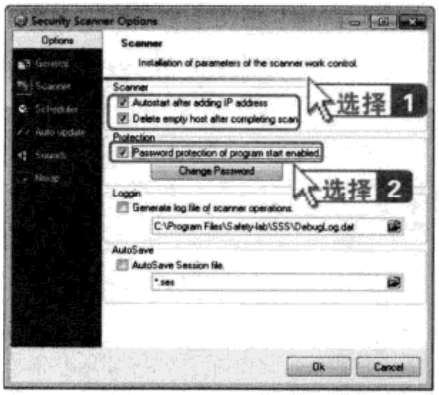

步骤2 打开【Security Scanner Options】窗口，该窗口主要有【General】、【Scanner】、【Scheduler】、【Auto update】、【Sounds】和【Nmap】6个选项。首先切换到【General】选项卡，该选项主要用来设置扫描速度，其中的“Threads”表示线程数，设置的线程数越大，扫描的速度越快，扫描的质量越低；“Modules”表示表示扫描的模块；“Total threads”表示总线程数。




步骤3 根据实际情况进行设置，设置完毕后切换到【Scanner】选项卡。

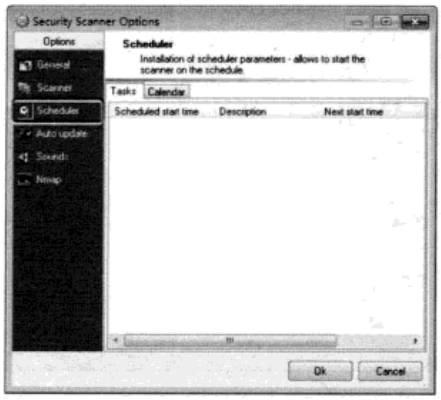



步骤4 选中【Autostart after adding IP address】和【Delete empty host after completing scan】复选框。在【Protection】组合框中选中【Password protection of program start enabled】复选框。

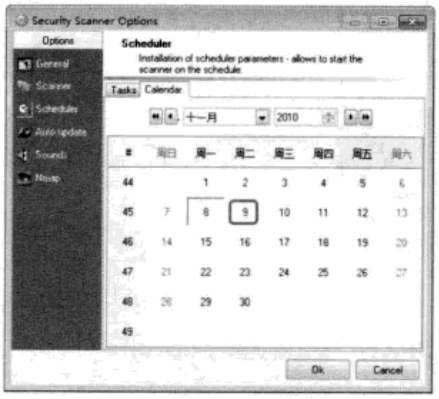



步骤5 打开一个对话框，要求用户输入密码，输入完毕后，单击 Ok 按钮即可。

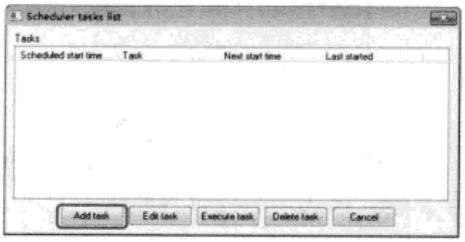

步骤6 密码设置完成后，切换到【Scheduler】选项卡，进入该选项的设置界面。




步骤7 切换到【Calendar】选项卡，可以看到一个日期面板。在此可以设置在某个日期要执行的具体任务。例如，在【月份】下拉列表中选择【十一月】选项，在【年份】微调框中选择【2010】，然后在下面的面板中双击日期【9】选项，即可设置2010年11月9日的任务。

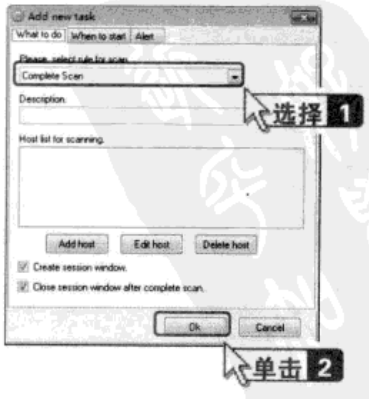



步骤8 弹出【Scheduler tasks list】对话框，单击 Add task 按钮。

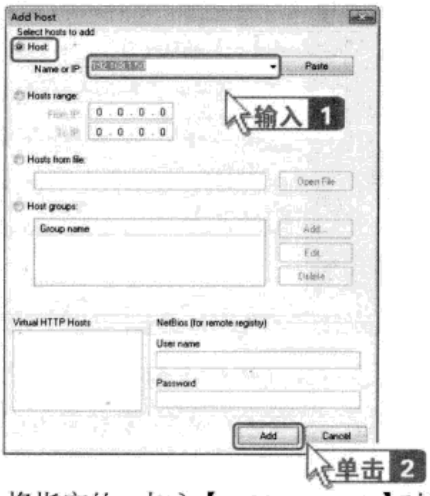



步骤9 弹出【Add new task】对话框，切换到【When to start】选项卡，可以在该选项卡中对任务的日期和时间进行设置。其中【Schedule task】下拉列表框中的“Once”表示执行一次任务；“Hourly”表示以小时为单位执行一次任务；“Daily”表示以天为单位执行一次任务；“Weekly”表示以周为单位执行一次任务；“Start time”表示任务开始执行的时间。

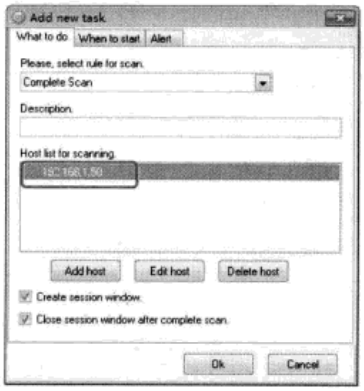

步骤10 切换到【What to do】选项卡，在【Please, select rule for scan】下拉列表中有很多选项。其中，“Complete Scan”表示完整扫描；“Full Scan”表示完全扫描；“Quick Scan”表示快速扫描；“Only NetBIOS Scan”表示只进行NetBIOS扫描；“Only FTP Scan”表示只进行FTP扫描；“Only HTTP Scan”表示只进行HTTP扫描，这里选择【Complete Scan】选项。然后单击 Add host 按钮。



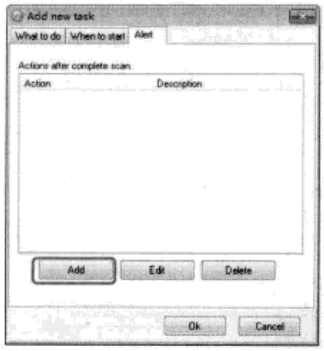
步骤11 打开【Add host】对话框，可以选中【Host】单选钮扫描一个固定IP，也可以选中【Hosts range】单选钮来设定扫描的主机范围。这里只对一个IP进行扫描，接着单击 Add 按钮。




步骤12 将指定的IP加入【Add new task】对话框中的【Hosting list for scanning】列表框中。

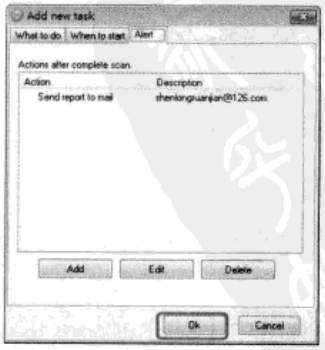



步骤13 切换到【Alert】选项卡，在该选项卡中没有任何信息，用户需要添加并设置此选项卡中的内容，添加好后单击 Add 按钮。

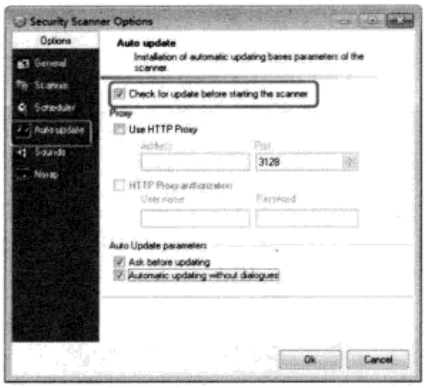



步骤14 打开【New Scheduler Action】对话框，在该对话框中设置相关的选项，设置完成后单击 Ok 按钮。

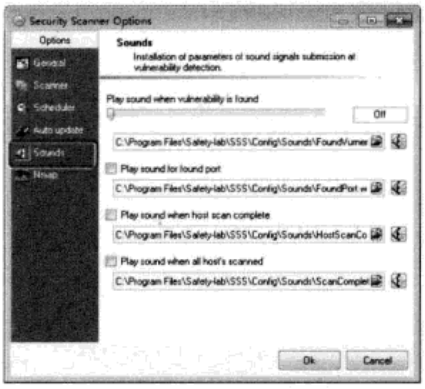

步骤15 返回【Add new task】对话框，然后单击 Ok 按钮即可完成设置。



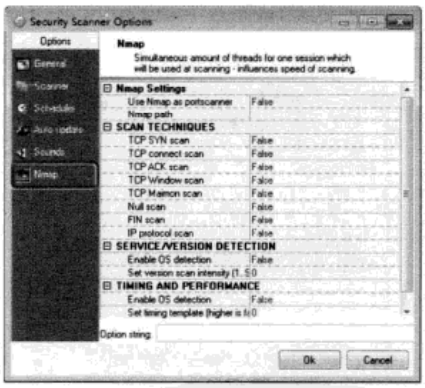
步骤16 返回【Security Scanner Options】窗口，选择左侧窗格中的【Auto update】选项，此时在右侧窗格中显示该选项的设置，因为SSS扫描器更新的频率非常快，所以建议选中【Check for update before starting the scanner】复选框。




步骤17 选择【Security Scanner Options】窗口中的【Sounds】选项，此时在右侧窗格中显示该选项的设置，主要用来设置发现端口、弱点时的提示声音。Play sound when vulnerability is found表示当发现漏洞就播放声音，拖动其下方的滑块可以改变声音的大小；Play sound for found port表示发现端口后播放的声音；Play sound when host scan complete表示完成主机扫描后播放声音；Play sound when all host's scanned表示所有的主机扫描完成后播放声音。需要注意的是：以上的所有操作中播放的声音都是可以更改的，用户只需要单击按钮即可选择其他的声音文件，但一定要正确选择声音文件的路径。




步骤18 设置完成后单击窗口左侧的【Namp】选项，各选项保持默认设置，接着单击 Ok 按钮即可完成【Option】功能选项的设置。

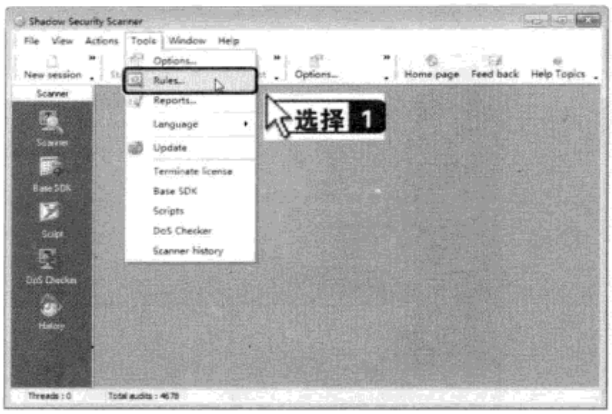


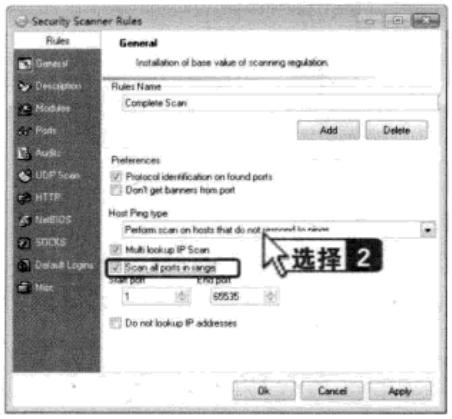

## 2. 【Rules】选项

下面介绍【Rules】选项的具体设置过程。

步骤1 打开SSS主窗口，然后选择【Tools】➤【Options】菜单项。

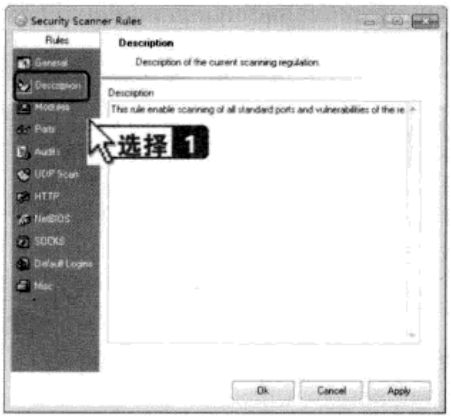
步骤2 打开【Security Scanner Rules】窗口，默认切换到【General】选项中，若用户需要进行详细的扫描，就要选中【Scan all ports in range】复选框，表示扫描所有的端口。

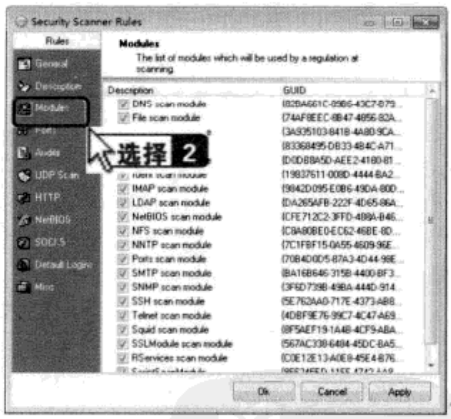



**步骤3** 在左侧窗格中选择【Description】选项，在右侧窗格中显示该选项的描述，用户可以自行描述，也可以采取默认描述。

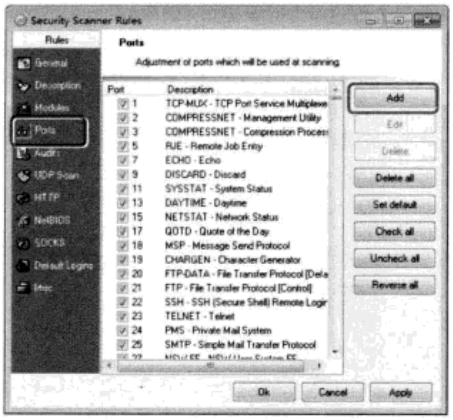
**步骤4** 切换到【Modules】选项界面，在右侧窗格中选中的选项越多，表示要扫描的模块就越多，扫描需要的时间就会相对地增加，但扫描的效果会更好一些，所以当对一台主机扫描时，建议将所有的复选框都选中。

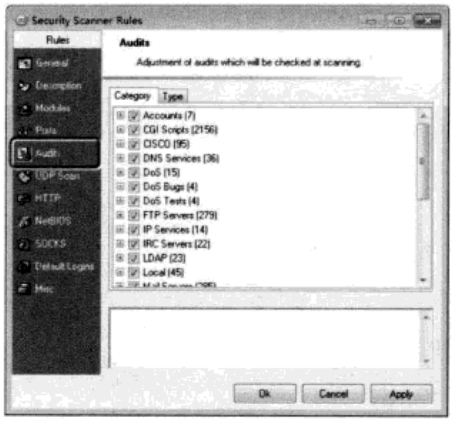



**步骤5** 切换到【Ports】选项界面，在右侧窗格中列出了所有常见端口及各端口的描述信息，用户也可以添加新的端口并给予描述，然后单击 Add 按钮，即可添加新的端口。

**步骤6** 在左侧窗格中选择【Audits】选项，在右侧窗格中选中所有复选框，其他的选项全都使用默认设置即可。



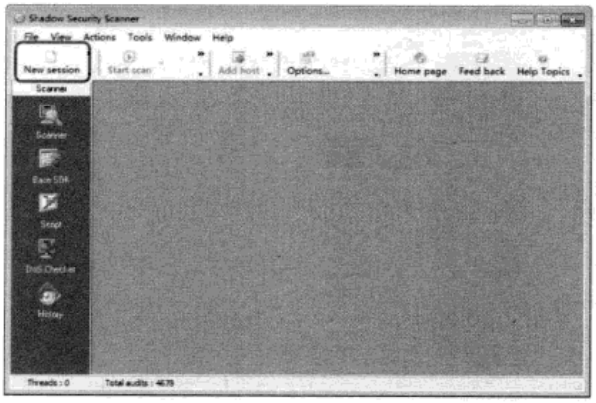




### 3. 操作实例

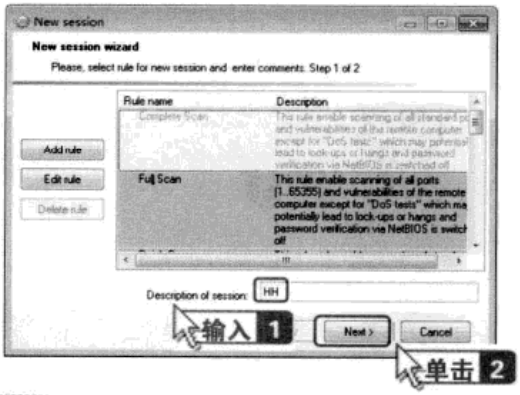
SSS最大的功能就是扫描漏洞。

对一台主机进行扫描的具体操作步骤如下。

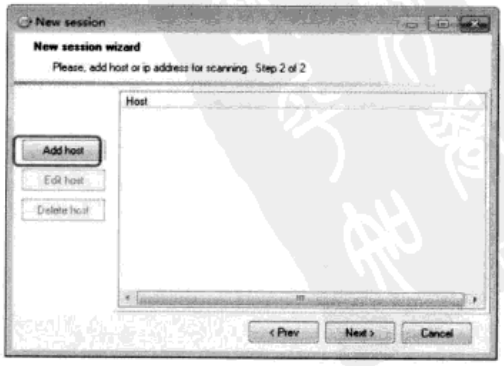
步骤1 打开SSS主窗口，并单击 New session 按钮。



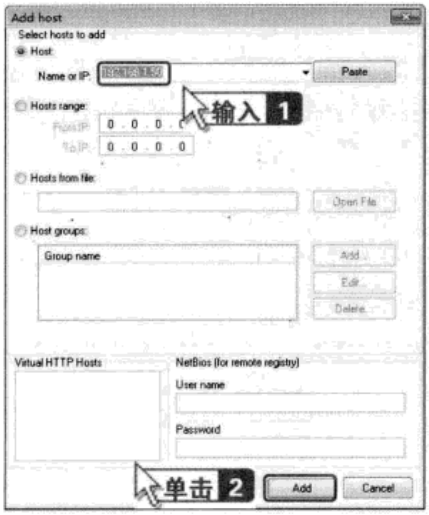

步骤2 打开【New session】窗口，按照前面介绍的方法对【Rules】选项进行设置，然后在【Description of session】文本框中输入对这次扫描的描述，这里输入“HH”，接着单击 Next > 按钮。



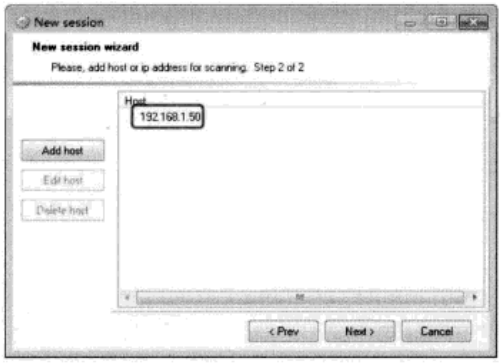

步骤3 打开添加扫描机器的窗口，单击 Add host 按钮。



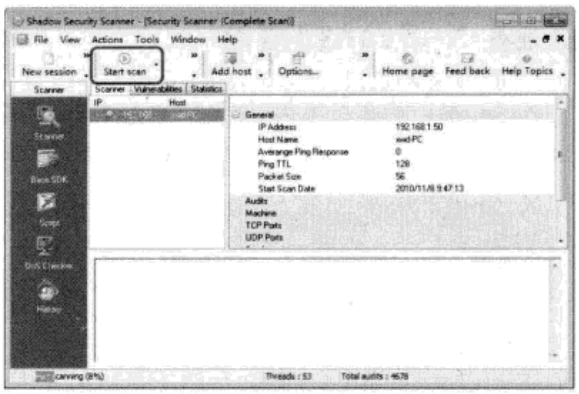
**步骤4** 打开【Add host】对话框，选中【Host】单选钮，在【Name or IP】文本框中输入主机名称或者IP地址。这里输入“192.168.1.50”，然后单击 Add 按钮。



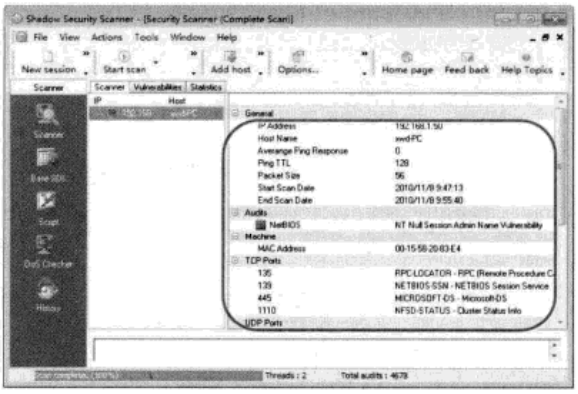

**步骤5** 返回【New session】窗口，此时可以看到【Host】列表框中已经添加了该IP地址。



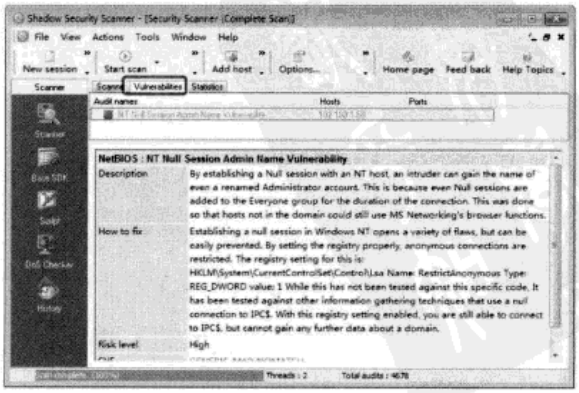

**步骤6** 单击 Next > 按钮进入下一个窗口，单击新窗口中的 Start scan 按钮，开始扫描。在下方的状态栏中显示了进度、线程以及总共需要检测的任务数。




**步骤7** 检测完成后在右侧的窗格中显示出检测结果，包括计算机的系统信息、共享信息、TCP及UDP开放端口等信息。




**步骤8** 切换到【Vulnerabilities】选项卡，单击扫描出来的漏洞，在该窗口的下侧显示该漏洞的描述、修复方法以及危险级别等信息。



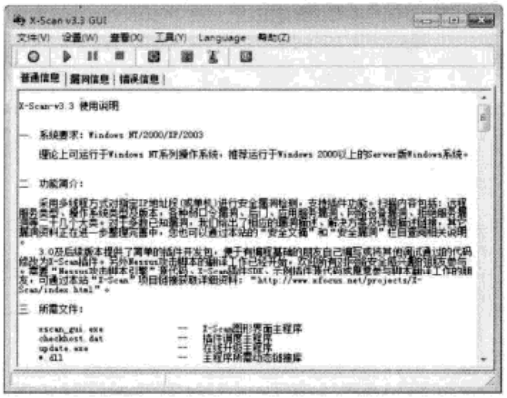
## 2.4.2 X-Scan扫描器

X-Scan是一款功能强大的安全漏洞扫描器，它能够准确地检测出用户计算机中的各种漏洞和弱口令等信息，是黑客常用的检测工具之一。

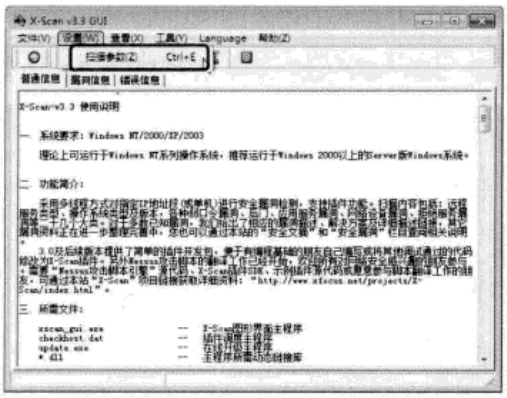
X-Scan采用多线程方式对指定的IP地址段或单机进行安全漏洞检测，检测内容包括操作系统类型和版本、远程服务类型、拒绝服务漏洞、应用服务漏洞和各种弱口令漏洞，同时还给出了相应的漏洞解决方案。一些黑客经常利用这款软件来检测用户计算机中的各种漏洞和弱口令，并对一些存在严重安全漏洞的用户进行入侵。

下面以X-Scan v3.3为例介绍这款软件的使用方法。具体的操作步骤如下。

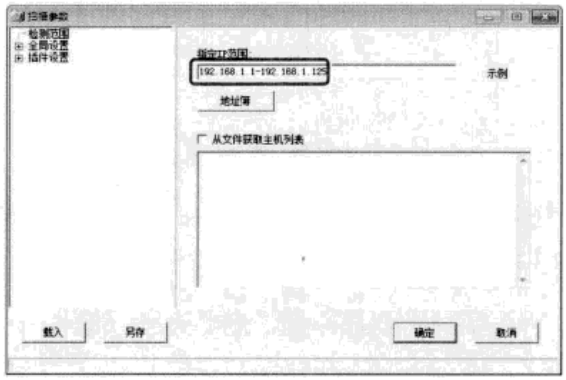
**步骤1** 下载X-Scan扫描器，然后运行该软件，打开其主界面。



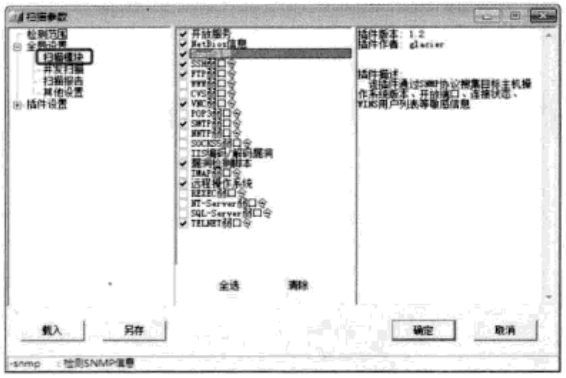
**步骤2** 在进行扫描之前，首先需要对扫描参数进行设置。选择【设置】➢【扫描参数】菜单项。



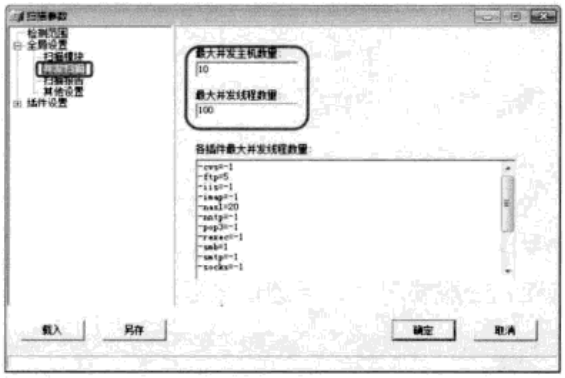
**步骤3** 打开【扫描参数】对话框，在【指定IP范围】文本框中输入IP地址范围。



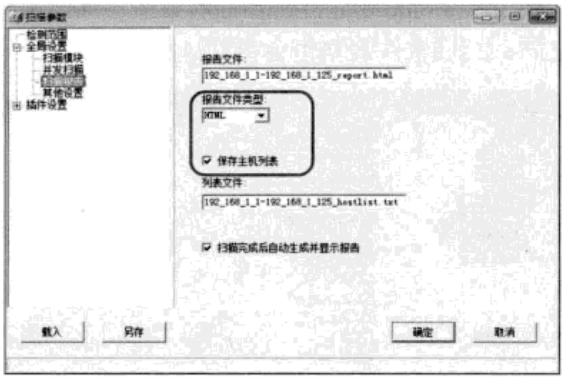
**步骤4** 单击左侧窗格中【全局设置】选项前面的⊞符号将其展开。选择【全局设置】➢【扫描模块】选项，在中间窗格中会显示该模块的具体内容，单击其中的任何一个插件，在右侧窗格中会显示关于该插件的描述，在此可以根据需要选中要扫描的插件。



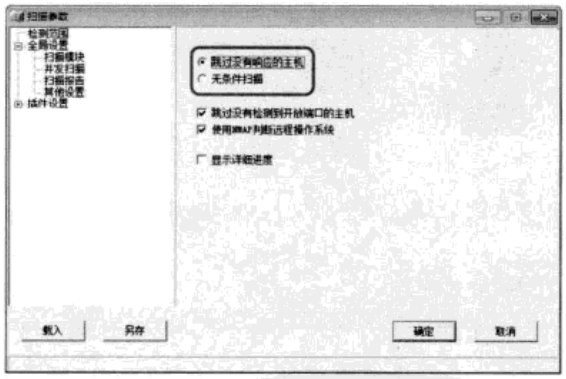
步骤5 设置完成后选择【并发扫描】选项，在右侧窗格的【最大并发主机数量】文本框中输入数量，在【最大并发线程数量】文本框中输入线程数，这些设置受硬件和宽带的影响，需要根据实际情况进行设置，一般情况下不要将线程设置得太大，以免影响扫描结果。



步骤6 并发主机数量和并发线程数量设置完成后选择【全局设置】➢【扫描报告】选项，在【报告文件类型】下拉列表中有【HTML】、【TXT】和【XML】3个选项，这里选择【HTML】选项，并选中【保存主机列表】复选框。

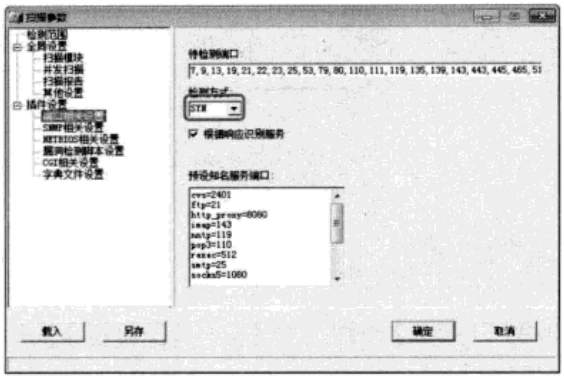


步骤7 选择【全局设置】➢【其他设置】选项，如果选中【跳过没有响应的主机】单选钮，则会先ping一下主机，如果没有相应，则跳过该主机。如果选中【无条件扫描】单选钮，就会强制扫描IP地址段中的每一台主机。这里可以根据需要进行选择。

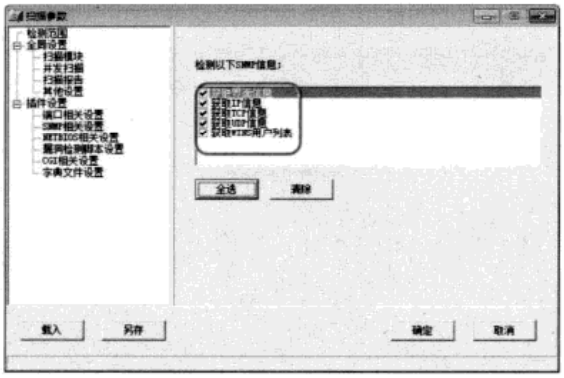


步骤8 选择完成后选择【插件设置】➢【端口相关设置】选项，在【待检测端口】文本框中可以添加一些端口，也可以删除一些不想检测的端口，对于普通用户来说，使用默认设置即可。同时还需要选择相应的检测方式，如果不想被扫描对象记录详细信息最好选择“SYN”方式，但该方式还是会在扫描对象的防火墙上留下扫描痕迹。检测方式选择完成后需要选中【根据响应识

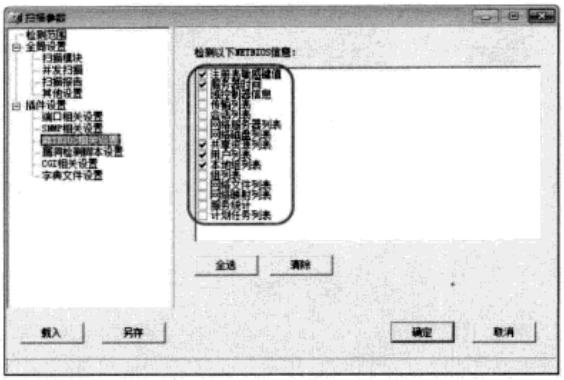
别服务】复选框，这样当扫描对象服务端口更改之后，扫描软件策略也会自动进行相应的调整。



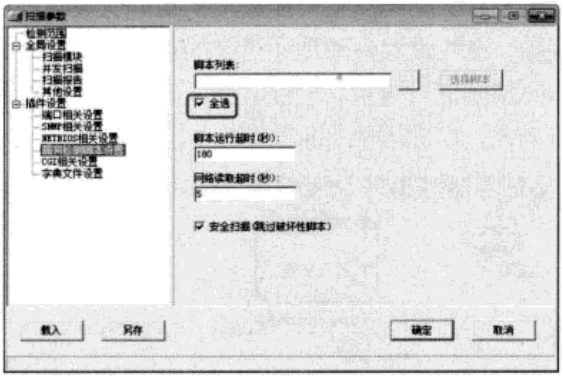
步骤9 选择【插件设置】➢【SNMP相关设置】选项，在右侧窗格中显示出需要检测的SNMP选项，可以根据需要进行选择。



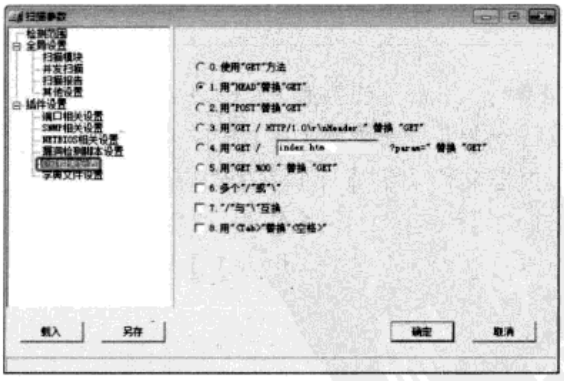
步骤10 选择【插件设置】➢【NETBIOS相关设置】选项，在右侧窗格中会显示出需要检测的NETBIOS信息，可以根据需要进行筛选。



步骤11 选择【插件设置】➢【漏洞检测脚本设置】选项，在右侧窗格中选中【全选】复选框。

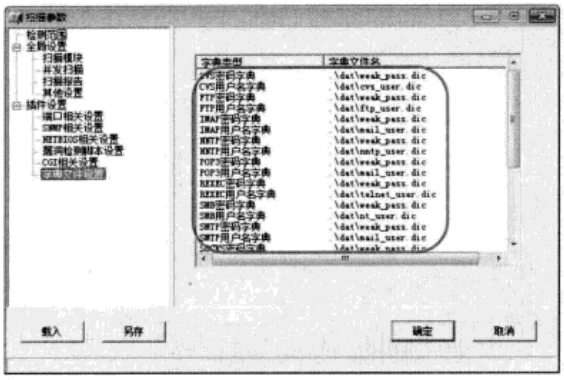


步骤12 选择【插件设置】➢【CGI相关设置】选项，一般情况下，该选项采取默认设置即可。

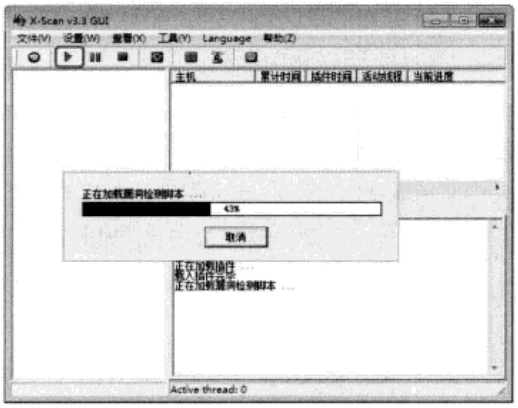


步骤13 选择【插件设置】➢【字典文件设置】

选项，在右侧的窗格中显示出各种类型的字典，这些字典都是内置的，用户也可以自行导入字典。



步骤14 设置完成后单击 确定 按钮，返回X-Scan主窗口，此时单击 ▶ 按钮即可进行扫描。在扫描过程中，在主界面中会显示出扫描出的普通信息、漏洞信息以及错误信息等。



步骤15 此扫描过程需要一段时间，扫描完成后会以页面形式弹出一个检测报告，此时在【主机列表】中发现局域网IP为192.168.1.122的计算机存在安全提示，单击【192.168.1.122】链接。

步骤16 跳至该主机的分析列表，单击【端口/服务】选项中的链接，可以跳至其安全漏洞和解决方案列表处进行查看，需要注意的是：如果检测的安全漏洞是用红色标记的，就说明该情况比较严重。

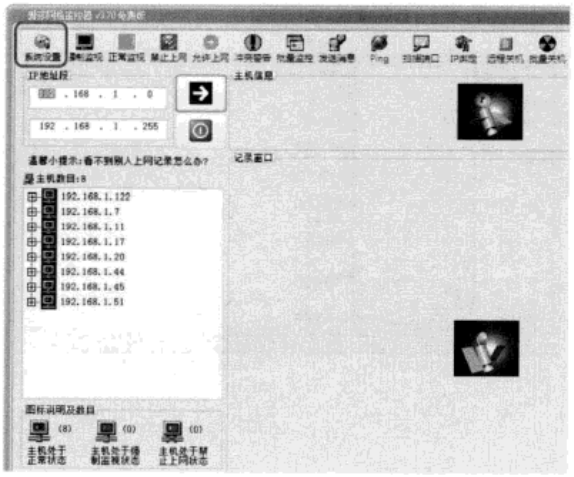
## 2.4.3 爱莎网络监控器

爱莎网络监控器是一款功能强大的网络监控软件，是企业的首选网络监控器，其操作简单、功能实用，可以实现对网页、QQ、MSN、FTP以及邮件收发等的监控，而且不需要在被监控和被管理计算机上安装任何软件，可以在网内任何一台计算机上安装。

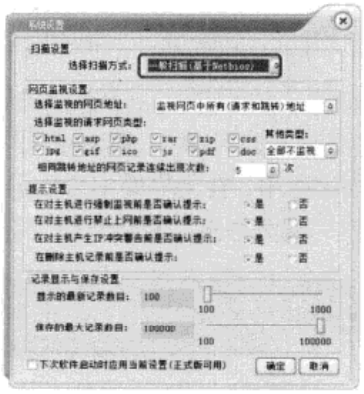
为了方便管理，用户在使用该软件之前需要对其进行设置。设置的具体步骤如下。

步骤1 启动爱莎网络监控器，弹出【选择网卡】对话框，这里采取默认设置即可。


步骤2 单击 确定 按钮，进入该软件的主窗口。由于受软件的限制，只能够截取核心设置部分，可以看到该软件的功能都在最上边的横栏中。首先单击【系统设置】按钮。

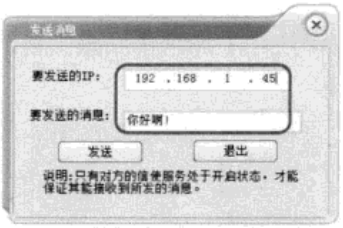



步骤3 弹出【系统设置】对话框。默认的扫描方式是【一般扫描（基于Netbios）】，用户也可以选择【高级扫描（基于Arp）】选项，该选项可以扫描到更多的存活主机，但它得不到目标主机的工作组和主机名等信息。其他选项采取默认设置即可。



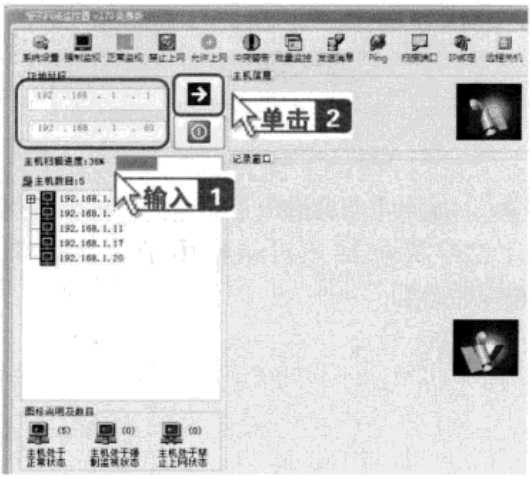

步骤4 单击 确定 按钮，返回主窗口，在工具栏处单击【批量监控】按钮。弹出【批量监控】对话框，在【请选择要进行的批量操作】下拉列表中选择要进行的操作，然后选中想要监控的计算机的IP地址。

**步骤5** 设置完成后单击 应 用 按钮，返回软件主窗口，然后单击【发送消息】按钮，弹出【发送消息】对话框，在【要发送的IP】文本框中输入想要发送消息的IP地址，在【要发送的消息】文本框中输入要发送的信息内容（需要注意的是：对方需要开启信使服务）。单击 发送 按钮，即可将消息发送到指定IP的计算机。单击 退出 按钮可返回主窗口。ping操作和扫描端口操作的方法相似，这里不再赘述。




在实际使用中会发现该监控器的功能十分强大，操作比较简单。下面通过一个实例介绍该软件的使用方法。

**步骤1** 运行该软件，默认的设置是扫描局域网内的所有计算机。假设用户只对IP最后一段为0~60的计算机进行扫描，就可以将IP段填写在【IP地址段】组合框中，然后单击【IP地址段】右侧的【开始】按钮进行扫描。




**步骤2** 一般情况下，用户的计算机会列在被扫描出的计算机的第一位，这里以IP为192.168.1.20为例进行操作，首先单击该IP地址前面的【+】标记将其展开，此时可以看到检测出的用户的一些网络信息。

**步骤3** 在该IP地址上单击鼠标右键，在弹出的快捷菜单中，用户可以通过选择相应菜单项，来对被监控的计算机进行强制监视、禁止上网、产生IP冲突警告、发送信息、扫描端口、远程关机/重启以及导入IP-MAC绑定库等操作。具体的使用方法这里不再介绍。

## 2.4.4 流光——扫描利器

流光是一款中文版的扫描工具，其功能强大，非常适合国内的黑客使用。

### 1. 流光软件的基本设置

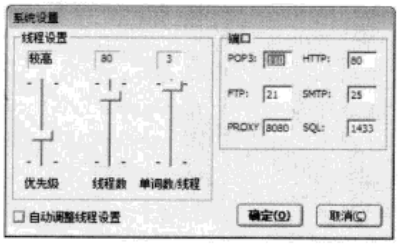
流光可以检测出POP3/FTP主机中的用户密码安全漏洞；采用多线程检测，消除系统的密码漏洞；可同时对多台POP3/FTP主机进行检测；阻塞线程具有自杀功能；支持10个字典同时检测；检测设置可作为项目保存等。在使用流光之前要先对其进行设置。

#### 【选项】菜单设置

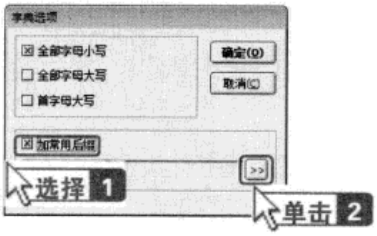
首先需要将流光软件安装到电脑上，具体的操作这里不再赘述。下面介绍如何对其【选项】菜单进行设置。

步骤1 启动流光软件，打开其主界面，选择【选项】➢【系统设置】菜单项。

步骤2 打开【系统设置】对话框，用户可以在此根据需求和硬件的配置来设置“优先级”、“线程数”以及“单词数/线程”，端口保持默认设置即可。



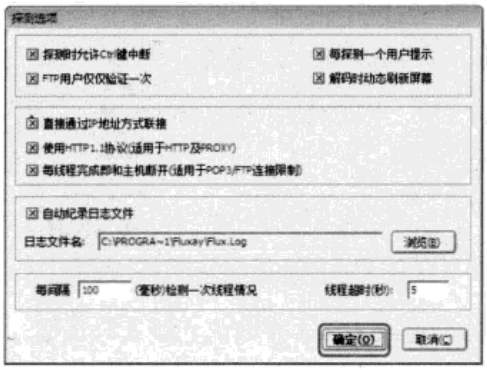
步骤3 单击 确定(O) 按钮返回主界面，选择【选项】➢【字典设置】菜单项，在弹出的【字典选项】对话框中选中【加常用后缀】复选框，然后单击 >> 按钮。



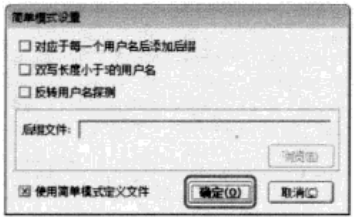

步骤4 弹出【打开】对话框，在【查找范围】下拉列表中选择【Fluxay】文件夹，在下方的列表框中选择【normal.suf】选项，然后单击 打开(O) 按钮。


步骤5 返回【字典选项】对话框，可以看到此文件已经添加到该对话框中了，然后单击 确定(O) 按钮。

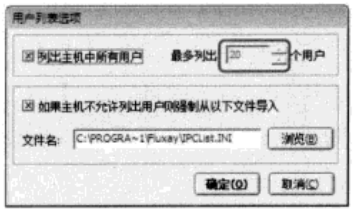

步骤6 返回主界面，选择【选项】➢【探测选项】菜单项，在弹出的【探测选项】对话框中选择适合的选项，并填写检测线程的间隔时间和线程超时时间。设置完成后单击 确定(O) 按钮。



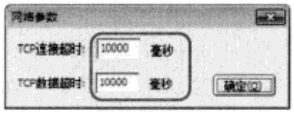

步骤7 返回主界面，选择【选项】➢【简单模式设置】菜单项，弹出【简单模式设置】对话框，这里采取默认设置，然后单击 确定(O) 按钮。



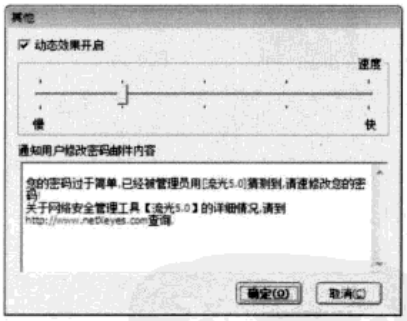

步骤8 返回主界面，选择【选项】➢【IPC用户列表选项】菜单项，弹出【用户列表选项】对话框。默认情况是列出20个用户，也可以增加或者减少用户个数。当需要列出所有的用户时，可以选中【列出主机中所有用户】复选框。




步骤9 单击 确定(O) 按钮返回主界面，选择【选项】➢【网络参数设置】菜单项，在弹出的【网络参数】对话框中设置【TCP连接超时】和【TCP数据超时】时间。默认设置为“10000毫秒”，用户可以适当地增加或减少。




步骤10 单击 确定(O) 按钮返回主界面，选择【选项】➢【其他】菜单项，弹出【其他】对话框。如果用户的计算机性能不是太高，可以取消选中【动态效果开启】复选框来关闭动态效果。

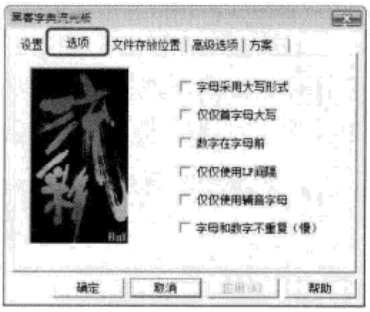



## 【工具】菜单设置

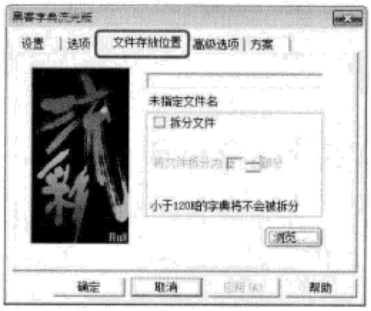
【工具】菜单中的菜单项很多，包括字典工具、NT/IIS工具、MSSQL、Fluxay Sensor工具以及远程网络嗅探等，用户可以自行实践和学习，这里主要介绍字典工具的设置。

步骤1 启动流光软件，打开其主界面，选择【工具】➢【字典工具】➢【字典工具Ⅲ－流光版】菜单项，弹出【黑客字典流光版】对话框，切换到【设置】选项卡，在此用户可以根据实际情况进行设置。

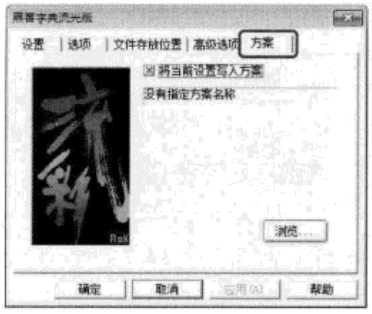

步骤2 切换到【选项】选项卡，在此选中合适的复选框。



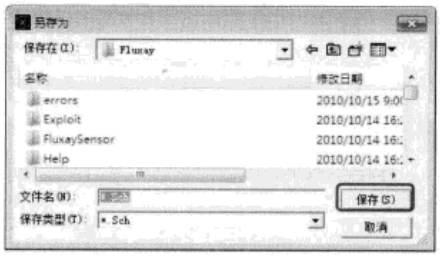

步骤3 切换到【文件存放位置】选项卡，在此可以指定文件的存放位置和文件名。




步骤4 切换到【方案】选项卡，选中【将当前设置写入方案】复选框。




步骤5 单击 浏览... 按钮，弹出【另存为】对话框，在【文件名】文本框中输入要保存的文件名，然后单击 保存(S) 按钮。

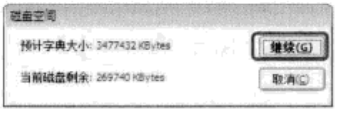



步骤6 返回【黑客字典流光版】对话框，单击 确定 按钮，在弹出的【字典属性】对话框中列出了该字典的所有信息。

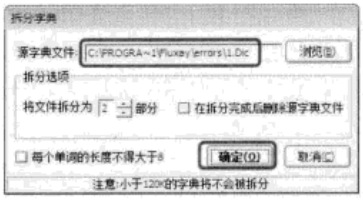

步骤7 单击 开始(S) 按钮，弹出【注意】对话框，提示用户字典成功生成。

**步骤8** 返回主界面，选择【工具】➤【字典工具】➤【根据拼音规则】菜单项，弹出【拼音规则】对话框，这里面的词根是汉语拼音的声母和韵母，单击...按钮添加需要保存的位置，设置完成后单击 确定(O) 按钮。

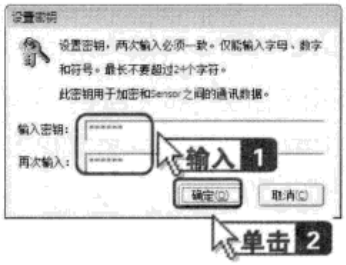

**步骤9** 弹出【磁盘空间】对话框，显示预计的字典大小，单击 继续(G) 按钮，生成与设置相对应的拼音字典。生成英语规则的字典与生成拼音规则的字典类似，这里不再赘述。



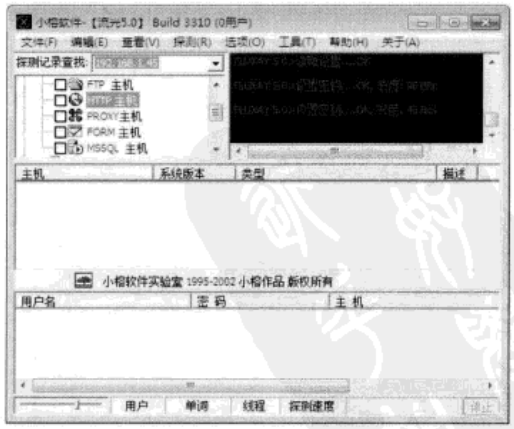

**步骤10** 选择【工具】➤【字典工具】➤【拆分字典】菜单项，弹出【拆分字典】对话框，单击 浏览(B) 按钮，添加需要拆分的字典文件，接着在【拆分选项】组合框中可以设置将文件拆分成几部分，然后单击 确定(O) 按钮即可。字典的合并和字典拆分类似，这里不再赘述。




**步骤11** 选择【工具】➤【设置加密密钥】菜单项来加密与Sensor之间的通信数据，从而保证其安全性，此时会弹出【设置密钥】对话框。在【输入密钥】文本框中输入要设置的密码，并在【再次输入】文本框中确认一次，然后单击 确定(O) 按钮。



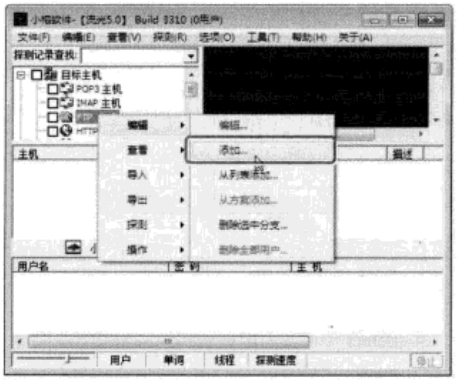

**步骤12** 返回主界面，此时会提示设置密钥成功，48表示6位密码，56表示7位密码，以此类推。需要注意的是：该软件中的密码至少要6位。



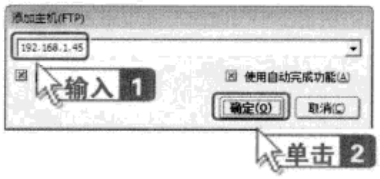

## 2. 流光软件的使用

下面介绍如何使用流光扫描一个FTP和HTTP的主机，具体的操作步骤如下。

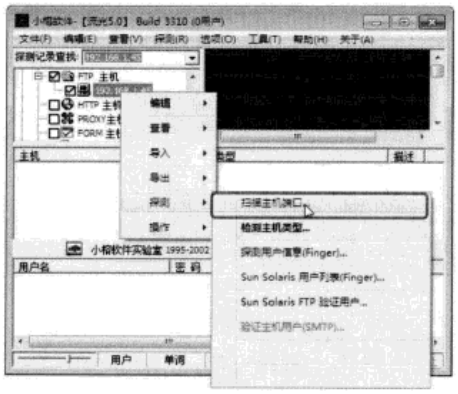
步骤1 启动流光软件，在主界面左侧的窗格中可以看到主机列表，选中【FTP主机】复选框，并单击鼠标右键，在弹出的快捷菜单中选择【编辑】➤【添加】菜单项。



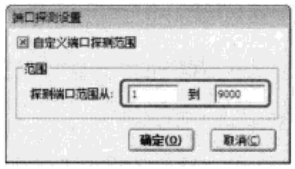
步骤2 弹出【添加主机（FTP）】对话框，在下拉列表中输入主机的域名或IP地址，然后 确定(O) 按钮。



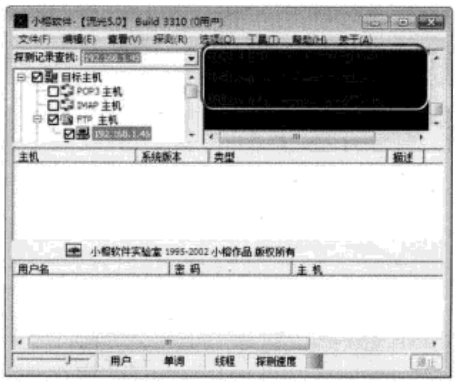

步骤3 此时会看到在【FTP主机】下面增加了刚刚添加的主机，接着选择该FTP服务器，然后单击鼠标右键，在弹出的快捷菜单中选择【探测】➤【扫描主机端口】菜单项。



步骤4 弹出【端口探测设置】对话框，选中【自定义端口探测范围】复选框可以自定义端口探测的范围（端口的范围为1~65535）。设置完成后单击 确定(O) 按钮。




步骤5 返回主界面，在右侧的窗格中可以看到扫描的过程。

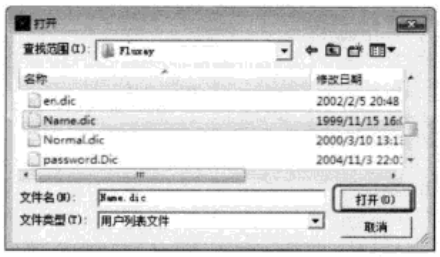


步骤6 稍等片刻，会弹出【探测结果】对话框，其中列出了开放的端口以及该端口的服务。单击 确定(O) 按钮，即可完成FTP主机端口的扫描。利用同样的方法可以对一个HTTP主机进行扫描，具体操作步骤这里不再赘述。

下面介绍如何进行一次简单模式的探测，具体的操作步骤如下。

**步骤1** 按照前面介绍的方法添加一个FTP主机，接着选择该主机，然后单击鼠标右键，在弹出的快捷菜单中选择【编辑】➢【从列表添加】菜单项。

**步骤2** 弹出【打开】对话框，此时字典就有用处了，在流光内部内置了很多字典，在这里选择内置的Name.dic字典进行探测，单击 打开(O) 按钮。




**步骤3** 这时字典文件就会自动导入该FTP主机下面（如果用户知道该FTP服务器的一个账户，也可以选择【编辑】➢【添加】菜单项将其单个导入）。选择【工具】➢【模式文件设定】➢【简单模式探测设置文件】菜单项。

**步骤4** 弹出【Single.INI−记事本】窗口，显示一些简单的密码（默认只有一个123456的密码，用户可以再添加一些密码）。


**步骤5** 添加好后保存并关闭窗口，返回流光的主界面，然后选择【探测】➢【简单模式探测】菜单项。稍等片刻，会显示探测结果，其中列出了开放的端口以及该端口的服务。

## 2.4.5 加壳与脱壳

加壳与脱壳工具是黑客常用的，通过这些工具可以对程序进行伪装和保护，从而降低被杀毒软件捕获的可能性，达到免杀的目的。

### 1. 加壳

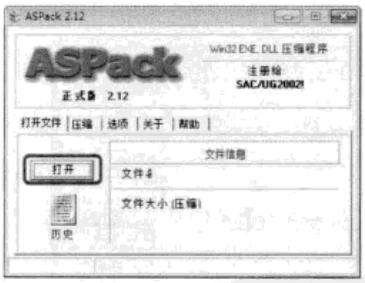
所谓加壳，是指通过一系列数学运算，对可执行程序文件或动态链接库文件的编码进行改变，以达到缩小文件体积或加密程序编码的目的。

加壳工具通常分为压缩壳和加密壳两类。压缩壳的特点是减小软件占用空间的大小，加密保护不是重点。目前兼容性和稳定性比较好的压缩壳工具有UPX、ASPack、ECompact等。加密壳种类比较多，不同的壳侧重点不同，一些壳只单纯保护程序，另外一些壳则提供额外的功能，如提供注册机制、使用次数、时间限制等。目前比较流行的加密壳有ASProtect、EXECrptor、Themida、EncryptPE、TTProtect、Armadilo等。

加壳的具体步骤如下。

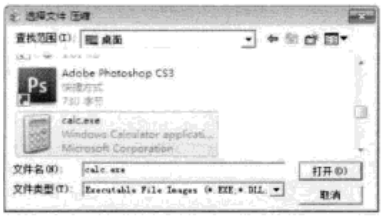
**步骤1** 启动ASPack软件，打开其主窗口，切换到【选项】选项卡，在此可以进行一些简单的设置。用户可以根据需要选中相应的复选框，也可以采用默认设置。

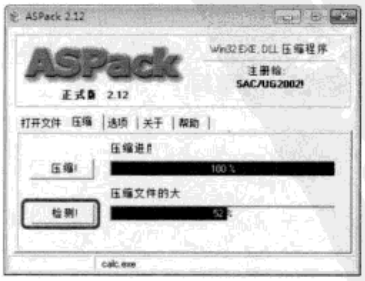
**步骤2** 切换到【打开文件】选项卡， 单击 打开 按钮。


**步骤3** 弹出【选择文件 压缩】对话框，在这里选择保存在桌面上的计算器程序。

**步骤4** 单击 打开(O) 按钮，即可切换到主窗口中的【压缩】选项卡进行加壳。



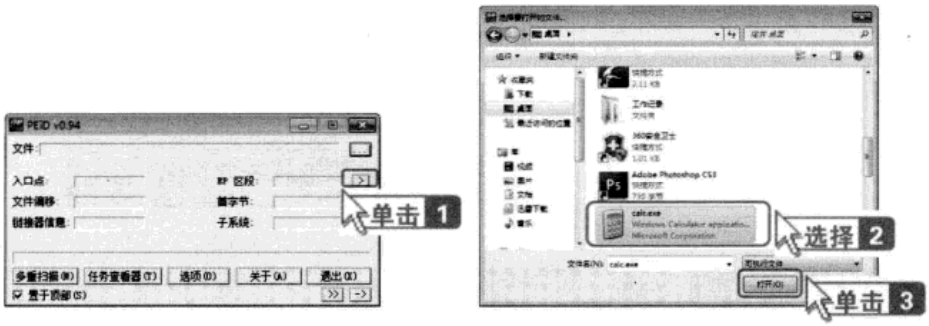



步骤5 当【压缩进度达到100%】时，说明已经成功地进行了加壳操作。单击 检测! 按钮对运行程序进行测试，并弹出【计算器】窗口。此时可以验证加壳后有没有影响到程序的运行。

前面介绍了程序加壳的方法，那么怎么知道一个程序有没有加过壳呢？这里就需要通过软件来检测，目前最常用的检测软件是PEID。通过PEID软件对可执行文件进行加壳检测的具体步骤如下。

步骤1 启动PEID，打开其主界面。

步骤2 单击 ... 按钮，弹出【选择要打开的文件…】对话框，这里仍然以计算器程序为例进行说明。然后单击 打开(O) 按钮。




步骤3 返回软件的主界面，显示已经检测到的信息。有编程经验的用户可以看出计算器程序是用VC++语言编写的，说明此刻没有进行加壳。

步骤4 对于普通用户来说，用PEID打开的程序如果已经加壳，就会看到下面框中有【->】符号，也就是说，只要出现了这个符号，就说明该程序加壳了，该符号的左边是所用加壳软件的名称和版本。

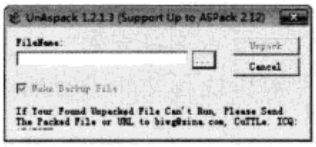

## 2. 脱壳

一般情况下，软件被加壳工具加壳后都可以找到相应的脱壳工具进行脱壳，因此只要找到与之相应的脱壳工具，绝大多数的壳都可以轻松地脱去。

例如，对应于ASPack加壳软件的脱壳软件是UnAspack（软件版本必须高于1.2.1.3，否则不支持ASPack V2.12）。下面介绍如何使用UnAspack软件对已被加壳的计算器程序进行脱壳，具体的操作步骤如下。

步骤1 启动UnAspack，打开其主界面。

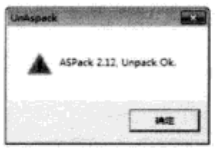
步骤2 单击...按钮，弹出【打开】对话框，选择加过壳的计算器程序，然后单击 打开(O) 按钮。

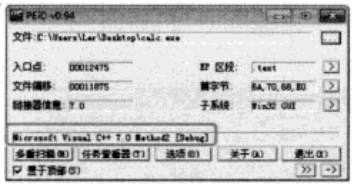




步骤3 返回软件的主界面，此时该程序的路径已经装载进了软件中，单击 Unpack 按钮，弹出【UnAspack】对话框，提示用户脱壳成功，单击 确定 按钮完成一次脱壳操作。

步骤4 此时再用PEID检测，可以发现该计算机程序已经没有壳了。




## 新手问题解答

### 如何制作一个加壳病毒并脱壳和检测

加壳和脱壳的工具很多，用户可以参照2.4.5中的内容，使用ASPack加壳软件和UnAspack脱壳软件来进行操作。

在加壳和脱壳过程中，用户还可以利用PEID软件进行检测。

### 如何查看本主机的 IP 地址和 MAC 地址

查看本主机的IP和MAC地址的方法很多。

在【命令提示符】中输入“ipconfig /all”，然后按下【Enter】键即可进行查看。

用户还可以打开【网络和共享中心】窗口，在其中单击【本地连接】链接，在弹出的【本地连接 状态】对话框单击【详细信息】按钮，在弹出的【网络连接详细信息】对话框中可以查看IP和MAC地址。

# 第3章
# 谁动了我的电脑

微软仿照人们大脑的记忆功能为计算机的视图操作系统设计了记忆功能。从启动登录记录，到程序运行记录，或者系统的变动情况，只要细细查看，都能找到蛛丝马迹。

**要点导航**

- ◎ 查看电脑的使用记录
- ◎ 查看系统记录
- ◎ 查看网页记录

# 3.1 查看电脑的使用记录

用户可以通过“事件查看器”来查看电脑的使用记录。下面介绍如何查看电脑的使用记录。

## 3.1.1 查看上网时间

在Windows 7系统中，通过“事件查看器”可以查看上网时间的具体步骤如下。

步骤1 在桌面上单击【控制面板】图标，弹出【控制面板】窗口，在其中查找到并双击【管理工具】图标。

步骤2 在弹出的【管理工具】窗口中查找并双击【事件查看器】图标。



步骤3 在左侧的窗格中选择【事件查看器（本地）】➢【Windows日志】➢【系统】选项，然后在右侧窗格的【系统】选项卡中选择【筛选当前日志…】选项。

步骤4 弹出【筛选当前日志】对话框，切换到【筛选器】选项卡，在【事件来源】下拉列表中选中【RemoteAccess】复选框，然后单击 确定 按钮，返回【事件查看器】窗口，在中间的窗格中就会显示出上网的开始时间和结束时间。


## 3.1.2 查看电脑开关机记录

在Windows 7系统中，用户可以通过“事件查看器”的“事件日志服务”来查看计算机的开、关机时间。因为“事件日志服务”会随计算机一起启动和关闭，并在事件日志中留下记录。

在“事件查看器”中的ID号为6006的事件表示事件日志服务已停止，如果当天在“事件查看器”中没有发现ID号为6006的事件，那么就表示计算机没有正常关机。当启动系统时，“事件查看器”的“事件日志服务”就会启动其ID号为6005的事件。

用户通过这两个ID号保存的信息能够很轻松地查看计算机的开、关机记录。具体的操作步骤如下。

步骤1 在桌面上双击【控制面板】图标，弹出【控制面板】窗口，在其中查找并双击【管理工具】图标，在弹出的【管理工具】窗口中，查找并双击【事件查看器】图标，接着在左侧的窗格中选择【事件查看器（本地）】➢【Windows日志】➢【系统】选项，在右侧的窗格中选择【筛选当前日志…】选项，弹出【筛选当前日志】对话框，切换到【筛选器】选项卡，在【事件来源】下拉列表中选中【eventlog】复选框，然后单击 确定 按钮。

步骤2 返回【事件查看器】窗口，在中间的窗格中显示出计算机的开、关机记录。

步骤3 在中间窗格的【系统】列表框中，分别单击【事件ID】为6005、6006的记录，然后在其下方的面板中可以看到其描述信息分别为“事件日志服务已启动”和“事件日志服务已停止”，分别表示计算机的开机时间和关机时间。

### 3.1.3 查看系统异常记录

用户还可以在“事件查看器”中找到系统异常记录，比如在某个时间段出现比较多的警告或错误信息。信息的内容大致如下。

事件类型：错误

事件来源：Winlogon

事件类别：无

事件ID：1015

用户：N/A

计算机：BILLGATES

描述：一个关键系统进程，C:\WINDOWS\system32\lsass.exe，失败，状态码是c0000005。必须现在重新启动机器。

上述的系统日志记录说明系统已经中毒。

“事件查看器”的应用很多，通过设置筛选器的事件来源，可以查看Windows中发生的很多事件的真实记录。

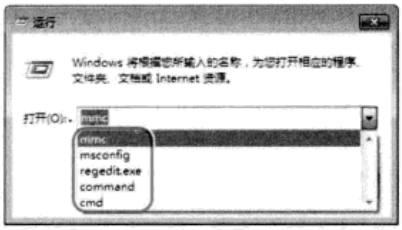
## 3.2 查看系统记录

查看系统记录也是查看黑客行迹很重要的一部分，下面介绍如何查看一些常见的系统记录。

### 3.2.1 查看程序运行记录

在Windows 7系统中，打开【运行】对话框，在其中的【打开】下拉列表中记录了用户运行过的命令。

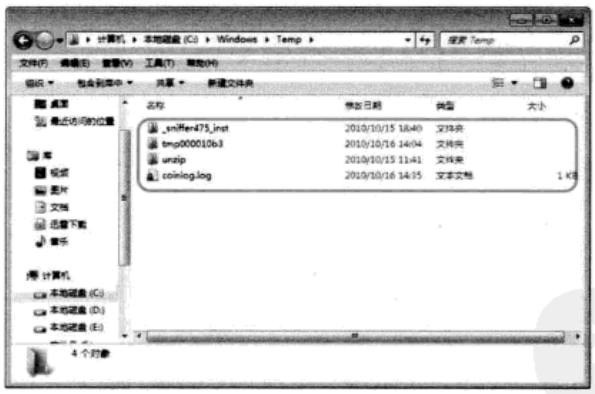
另外，与这个下拉列表对应，在注册表的HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU下也记录了用户运行过的命令。





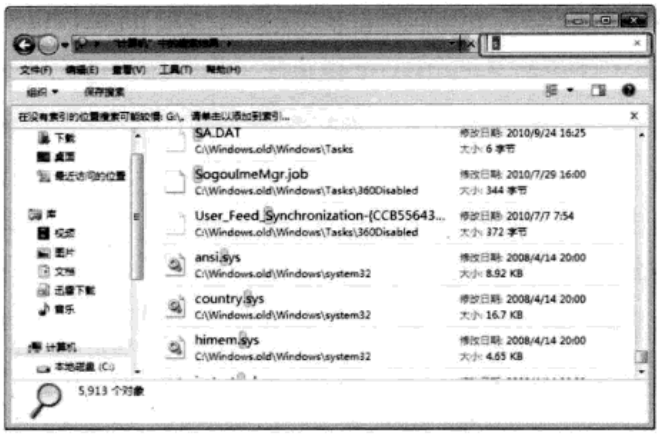
## 3.2.2 查看TEMP文件夹记录

TEMP文件夹用来存储临时文件，解压缩或安装新程序时都会生成临时文件，并且有很多文件并不会随程序关闭而删除。例如，在使用Office时，Word会产生临时文件和恢复文件，从中可以知道用户曾经操作过的文档，甚至可以从临时文件里恢复文档的内容。在Windows 7中，TEMP文件夹位于C:\Windows文件夹下。




## 3.2.3 查看Windows搜索记录

在Windows 7系统中，查看Windows搜索记录非常简单，首先在桌面上双击【计算机】图标，弹出【计算机】窗口，在右上角的【搜索栏】文本框中输入一个“引子”，例如，如果之前搜索过“svchost”文件，则需要输入一个“s”进行引导，此时所有以“s”开头的文件名或关键词都会完全显示出来，并自动进行搜索。

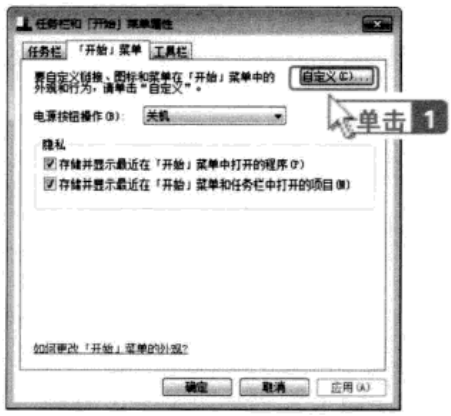


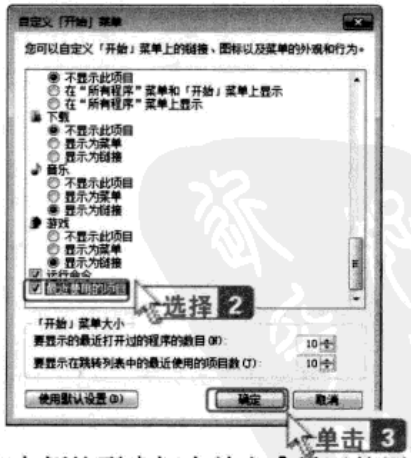

## 3.2.4 查看【开始】菜单中的文档记录

在Windows 7系统中，通常情况下，【开始】菜单中没有“最近使用的项目”。用户需要通过设置才可以找到它，并且可以通过它来查看用户最近调用了计算机中的哪些文档。具体的操作步骤如下。

步骤1 在Windows 7系统桌面上右键单击【开始】菜单按钮，在弹出的快捷菜单中选择【属性】选项，弹出【任务栏和「开始」菜单属性】对话框，切换到【「开始」菜单】选项卡，然后单击 自定义(C)... 按钮。

步骤2 弹出【自定义「开始」菜单】对话框，在其下方的列表框中找到并选择【最近使用的项目】复选框，然后单击 确定 按钮。




步骤3 返回桌面，单击【开始】菜单按钮，然后在右侧的列表框中单击【最近使用的项目】选项即可查看最近使用的项目。


## 3.2.5 查看回收站

在Windows系统中删除的文件会暂时放在回收站中，如果想找回误删的文件，只要回收站没有被清空，就有可能在回收站中找到误删的文件。在回收站中右键单击要还原的文件，从弹出的快捷菜单中选择【还原】菜单项，便可以找回。而且即使清空了回收站，借助一些数据恢复软件也能够把被删除的文件复原。


## 3.2.6 查看添加删除程序记录

软件安装后，控制面板的【程序和功能】界面会多出一个安装软件的条目：如果有软件被删除，也会少相应的条目。【程序和功能】中的当前安装程序列表对应注册表中的HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall键。


## 3.2.7 查看注册表编辑器记录

Windows 7系统的注册表具有记忆功能，在打开注册表时会自动定位到上次运行注册表时最后打开的键。

但是，让注册表“失忆”的方法也很简单，只要将注册表定位到“HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Applets\Regedit”项，右键单击该选项，在弹出的快捷菜单中选择【权限】选项，在打开的【权限】对话框中设置【完全控制】和【读取】选项为“拒绝”。



这样注册表编辑器的记忆功能就被禁止了。不过使用这种方法，注册表编辑器的收藏夹功能也同时被禁止，给日常编辑注册表带来不便。这时可以先在“HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Applets”项下新建一个Favorites项，然后再按上面的方法将Regedit项的权限设为拒绝，这样既可禁止注册表编辑器的记忆功能，又不会影响收藏夹的使用。


## 3.3 查看网页记录

在Windows中的各种软件中，留下记录最多的是IE浏览器。

### 3.3.1 查看Cookies聊天记录

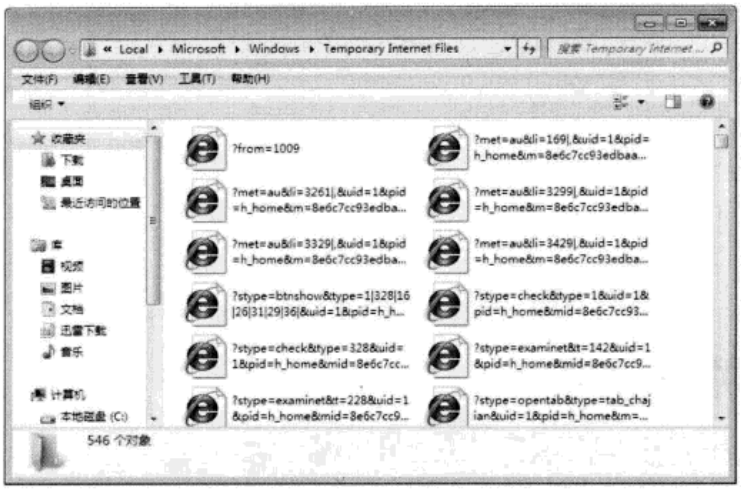
Cookies不是IE浏览器产生的，而是用户浏览的网站服务器发送出来的，并通过浏览器在用户的计算机硬盘存储少量的数据。这些数据主要是一些标识码，记录了用户在Web站点的访问次数、访问时间和进入站点的路径等信息。

Cookies可以加快用户浏览网页的速度。另外，有些网站还据此统计用户信息，可以为用户定制个性化服务，可以在用户不键入用户名和密码的情况下直接进入曾经浏览的某些站点。但是，有些恶意站点也会通过Cookies给用户制造一些小麻烦。查看Cookies的具体步骤如下。

步骤1 打开IE浏览器，在菜单栏上选择【工具】➢【Internet选项】菜单项，弹出【Internet选项】对话框，切换到【常规】选项卡，在【浏览历史记录】组合框中单击 设置(S) 按钮。

步骤2 弹出【Internet临时文件和历史记录设置】对话框，单击 查看文件(V) 按钮。

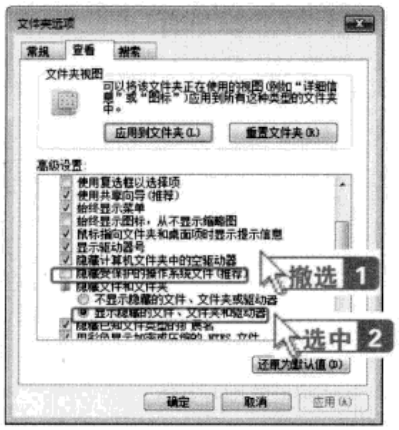
步骤3 打开保存Cookies文件的窗口，可以在该窗口中把不希望留下的Cookies删除。

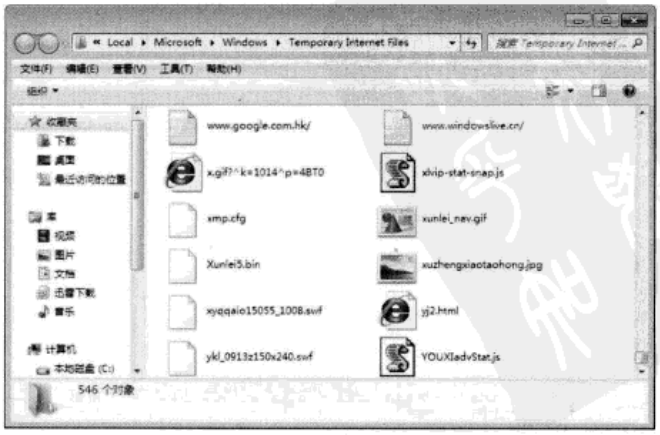



## 3.3.2 查看Internet临时文件记录

在查看Internet临时文件记录之前，需要先打开【计算机】窗口，选择【工具】➢【文件夹选项】菜单项，在弹出的【文件夹选项】对话框中，切换到【查看】选项卡，在【高级设置】列表框中取消选中【隐藏受保护的操作系统文件（推荐）】复选框，并选中【显示隐藏的文件、文件夹和驱动器】单选钮，然后单击 确定 按钮即可。

Internet临时文件与Cookies在同一个目录下，在Windows 7系统中默认位置是“C:\Users\Ler\AppData\Local\Microsoft\Windows\Temporary Internet Files”（其中Ler是账户名，C是系统安装盘符）。从这文件夹中可以看到IE浏览器产生的图片文件、HTML文件、JavaScript文件、Flash文件、下载的压缩文件和应用程序、ico图标文件等类型的文件。另外，也会有一些脚本病毒放在这里。



### 3.3.3 查看网页历史记录

历史记录保存了设置期限内用户浏览过的所有网站的记录，默认保存的位置是“C:\用户\Ler\AppData\Local\Microsoft\Windows\History”（其中Ler是账户名，C是系统安装盘符）。

在查看之前先在【文件夹选项】对话框中，取消选中【隐藏受保护的操作系统文件（推荐）】复选框和选中【显示隐藏的文件、文件夹和驱动器】单选钮。

打开【Internet选项】对话框，切换到【常规】选项卡，在【浏览历史记录】组合框中单击 设置(S) 按钮，在弹出的【Internet临时文件和历史记录设置】对话框中的【历史记录】组合框中设置历史记录保存的天数。



## 新手问题解答

### 如何查看剪贴板查看器记录

剪贴板查看程序是Windows自带的一个剪贴板操作工具，使用它可以对剪贴板中的数据进行浏览和简单的编辑。

选择【开始】➢【所有程序】➢【附件】➢【系统工具】➢【剪贴板查看程序】菜单项可以打开剪贴板查看程序并进行查看。

如果在Windows中没有这个程序，可以打开【控制面板】窗口，找到并双击打开【程序和功能】窗口，然后在打开的【打开或关闭Windows功能】对话框中进行添加即可。

如果用户在最后一次操作中复制的是一些敏感内容，一定要将剪贴板清除。

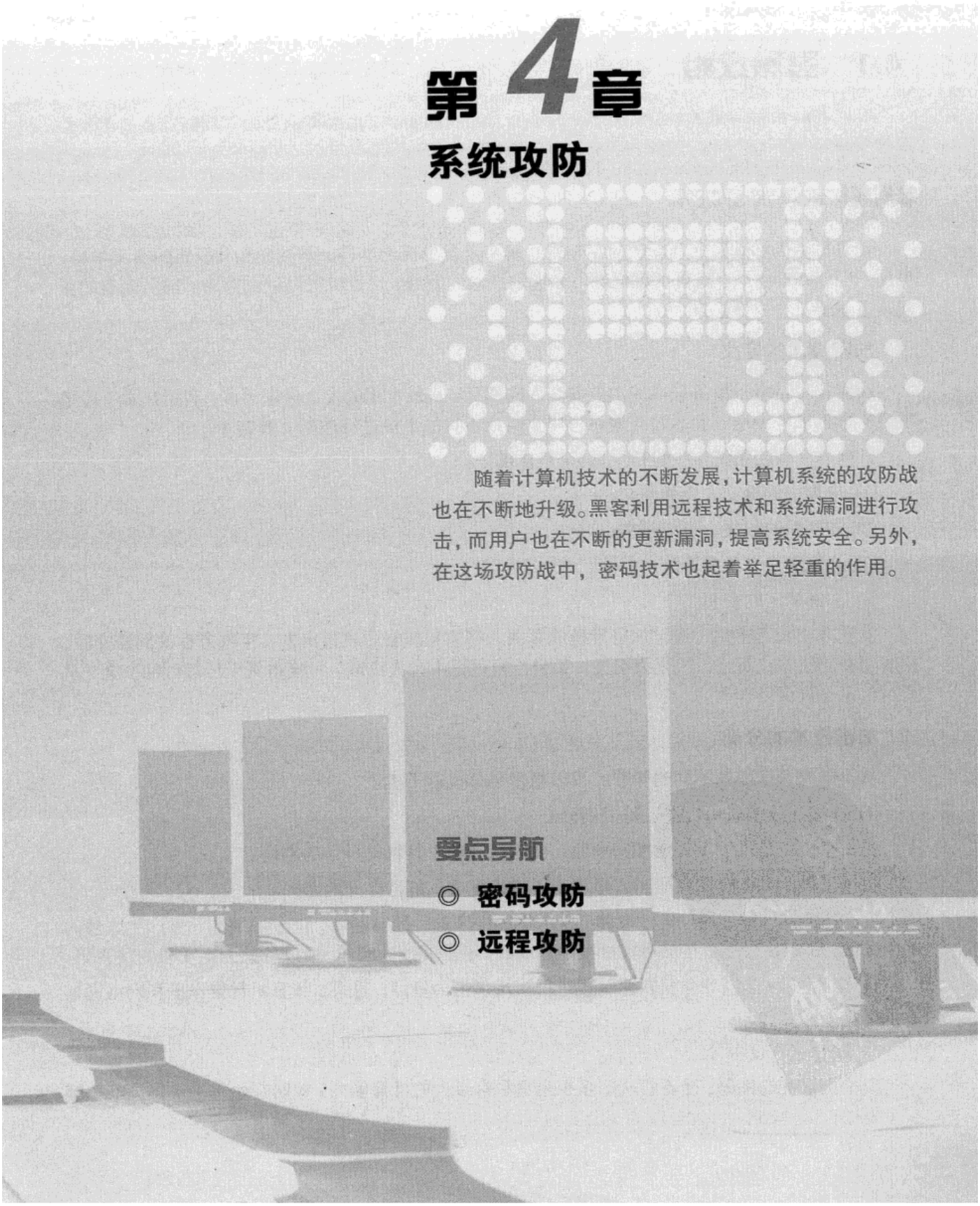
## 如何查看 QQ 聊天记录

用户可以通过QQ聊天记录查看工具来查看QQ的聊天记录。

在Windows 7系统中，QQ用户的个人信息都保存在“我的文档”中。

# 第4章 系统攻防

随着计算机技术的不断发展，计算机系统的攻防战也在不断地升级。黑客利用远程技术和系统漏洞进行攻击，而用户也在不断的更新漏洞，提高系统安全。另外，在这场攻防战中，密码技术也起着举足轻重的作用。



**要点导航**

- ◎ 密码攻防
- ◎ 远程攻防

# 4.1 密码攻防

加密和解密就像是矛和盾，加密是为了信息系统的安全，而解密则是为了攻破加密技术所建造的堡垒。

## 4.1.1 认识加密技术

计算机密码学是研究计算机信息加密、解密以及变换的学科，是数学和计算机的交叉学科，也是一门新兴的学科。随着计算机网络和通信技术的发展，计算机密码学也得到了前所未有的重视并迅速普及和发展起来。

### 1. 加密技术的定义

加密技术是电子商务采取的主要安全保密措施，是最常用的安全保密手段，利用技术手段把重要的数据加密传送，到达目的地后再用相同或不同的手段进行还原（解密）。

任何一个加密系统至少包括下面4个组成部分：

(1) 未加密的报文，也称明文；

(2) 加密后的报文，也成密文；

(3) 加密解密设备或算法；

(4) 加密解密的密钥。

发送方用加密密钥，通过加密设备或算法，将信息加密后发送出去。接收方在收到密文后，用解密密钥将密文解密，恢复为明文。如果传输过程中有人窃取，只能得到无法理解的密文，从而对信息起到保密作用。

### 2. 加密技术的分类

从不同的角度根据不同的标准，可以把密码分成若干类。

(1) 按应用技术或历史发展阶段划分。

手工密码：是以手工完成加密作业，或者以简单工具辅助操作的密码。

机械密码：是以机械密码机或电动密码机来完成加解密作业的密码。

电子机内乱密码：通过电子电路，以严格的程序进行逻辑运算，以少量制乱元素产生大量的加密乱数，因为其制乱是在加解密过程中完成的，不需要预先制作，所以称其为电子机内乱密码。

计算机密码：是以计算机软件编程进行算法加密为特点，适用于计算机数据保护和网络通信等广泛用途的密码。

(2) 按保密程度划分。

理论上保密的密码：是不管获取多少密文和有多大的计算能力，对明文始终不能得到唯一解

的密码，也叫理论不可破的密码。例如，客观随机一次一密的密码就属于这种。

实际上保密的密码：是在理论上可破解，但在目前的客观条件下，无法通过计算来确定唯一解的密码。

不保密的密码：是在获取一定数量的密文后可以得到唯一解的密码。例如，早期的单表代替密码，后来的多表代替密码，以及明文加少量密钥等密码，都属于不保密的密码。

(3) 按明文形态划分。

模拟型密码：用于加密模拟信息。例如，对动态范围内连续变化的语音信号加密的密码。

数字型密码：用于加密数字信息。是对两个离散电平构成0、1二进制关系的电报信息加密的密码。

(4) 按编制原理划分。

按编制原理，可以把密码分为移位、代替和置换3种，以及它们的组合形式。移位、代替和置换这3种原理在密码编制和使用中相互结合，灵活应用。

(5) 按密钥方式划分。

按密钥方式，可以将密码分为对称密码和非对称密码。

对称密码的特点是文件加密和解密使用相同的密钥，这种方法在密码学中叫做对称加密算法。这种算法使用起来简单快捷，密钥较短，且破译困难。数据加密标准（DES）和国际数据加密算法（IDEA）就属于对称密码。

非对称密码是为了解决信息公开传送和密钥管理问题，允许在不安全的媒体上的通信双方交换信息，安全地达成一致的密钥。这种算法需要两个密钥：公开密钥和私有密钥。公开密钥和私有密钥是一对，如果用公开密钥对数据进行加密，只有用对应的私有密钥才能解密；如果用私有密钥对数据进行加密，那么只有用对应的公开密钥才能解密。因为加密和解密使用两个不同的密钥，所以这种算法叫做非对称加密算法。

### 3. 常见的加密算法

现在的加密算法很多，公开的常用加密算法主要有DES、RSA、MD5等，下面分别介绍这几种算法。

(1) DES算法。

DES算法属于密码体制中的对称密码，又被称为美国数据加密标准，是1972年由美国IBM公司研制的对称密码体制加密算法。

采用DES算法时，明文按64位进行分组，密钥长64位，密钥事实上是56位参与DES运算（第8、16、24、32、40、48、56、64位是校验位，使得每个密钥都有奇数个1）。分组后的明文组和56位的密钥按位替代或交换的方法形成密文组。

DES加密算法的特点是分组比较短，密钥太短，密码生命周期短，运算速度较慢。

DES的入口参数有3个：key、data、mode。key为加密解密使用的密钥，data为加密解密的数据，mode为其工作模式。当为加密模式时，明文按照64位进行分组，形成明文组，key用于对数据加密；当为解密模式时，key用于对数据解密。实际运用中，密钥只用到了64位中的56位，这样才具有较高的安全性。

(2) RSA算法。

RSA算法是第一个能同时用于加密和数字签名的算法，也易于理解和操作。

RSA是被研究得最深入的公钥算法，是目前最优秀的公钥方案之一。RSA的安全性依赖于大数的因子分解，但并没有从理论上证明破译RSA的难度与大数分解难度等价，即RSA的主要缺陷是无法从理论上把握保密性能如何。

RSA的缺点主要有：产生密钥很麻烦，受到素数产生技术的限制，因而难以做到一次一密；分组长度太长，为保证安全性，至少也要600位以上，运算代价很高，尤其是速度较慢，较对称密码算法慢几个数量级，而且随着大数分解技术的发展，这个长度还在增加，不利于数据格式的标准化。

RSA算法是一种非对称密码算法，该算法涉及3个参数：$n$、$e1$、$e2$。

其中，$n$是两个大质数$p$、$q$的积，$n$的二进制表示所占用的位数，就是所谓的密钥长度。

$e1$和$e2$是一对相关的值，$e1$可以取任意值，但要求$e1$与（$p-1$）×（$q-1$）互质；再选择$e2$，要求（$e2 \times e1$）mod（$p-1$）×（$q-1$）=1[（$n$及$e1$），（$n$及$e2$）就是密钥对]。

RSA加解密的算法完全相同，设A为明文，B为密文，则A=B^$e1$ mod $n$，B=A^$e2$ mod $n$。$e1$和$e2$可以互换使用，即A=B^$e2$ mod $n$，B=A^$e1$ mod $n$。

(3) MD5算法。

MD5的全称是Message-Digest Algorithm 5（信息-摘要算法），是经MD2、MD3和MD4发展而来。它的作用是让大容量信息在使用数字签名软件签署私人密钥前被“压缩”成一种保密的格式（就是把一个任意长度的字节串变换成一定长度的大整数）。不管是MD2、MD4还是MD5，它们都需要获得一个随机长度的信息并产生一个128位的信息摘要。

## 4.1.2 系统加密

为了保护计算机中数据的安全，用户需要设置系统加密。系统加密一般有两种方法，分别是设置COMS开机密码和设置Windows启动密码。

### 1. 设置 CMOS 开机密码

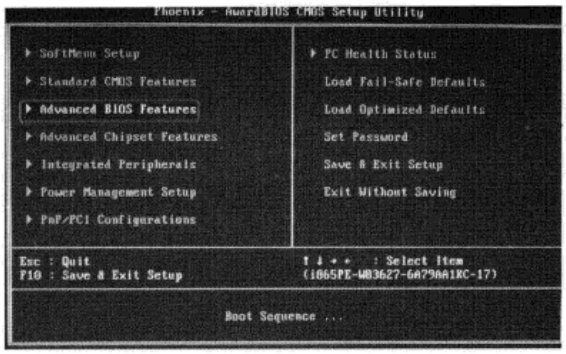
计算机在启动时首先要进行CMOS自检，然后才会进入操作系统，如果在CMOS中设置了开机密码，那么用户必须输入CMOS密码才能够继续计算机的启动。如果想要进入BIOS设置界面也必须输入密码，否则无法登录到系统中。因此可以通过设置CMOS开机密码来阻止别人进入

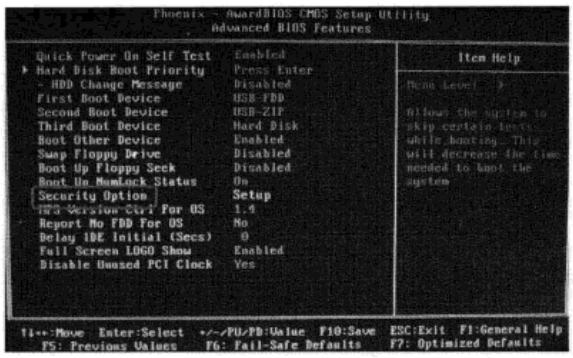
BIOS设置界面。

设置CMOS开机密码的步骤如下。

步骤1 在计算机启动过程中按下键盘上的【Del】键，进入BIOS设置界面。利用键盘上的方向键将光标移动到【Advanced BIOS Features】选项上，按下键盘上的【Enter】键。

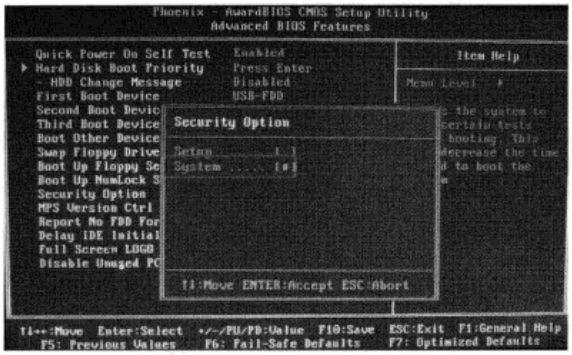
步骤2 进入【Advanced BIOS Features】选项的设置界面，将光标移动到【Security Option】选项上，按下【Enter】键。

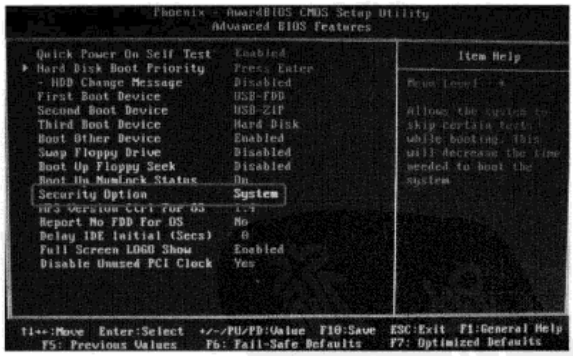



步骤3 进入【Security Option】选项的设置界面，将光标移动到【System】选项上，然后按下【Enter】键。

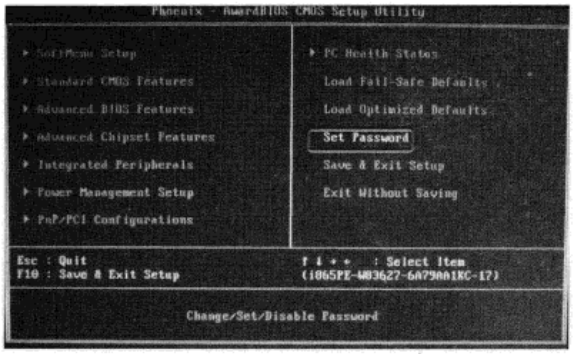
步骤4 返回【Advanced BIOS Feature】选项的设置界面，此时【Security Option】选项的默认值已经变为【System】，然后按下【Esc】键返回BIOS设置主界面。

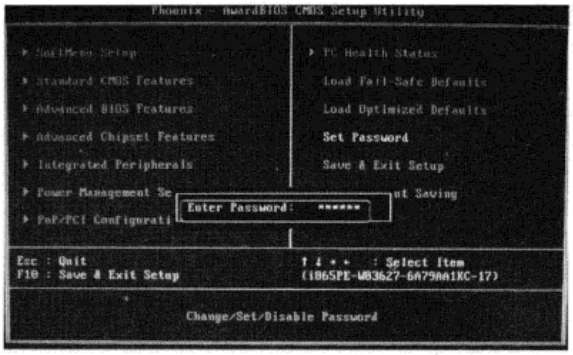



步骤5 利用键盘上的方向键将光标移动到【Set Password】选项上，按下【Enter】键。

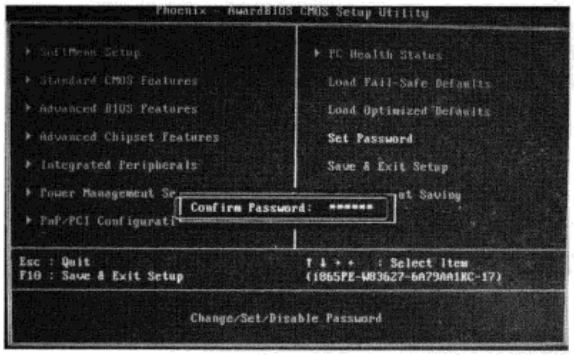
步骤6 在弹出的对话框中设置一个密码，输入完毕后再次按下【Enter】键。

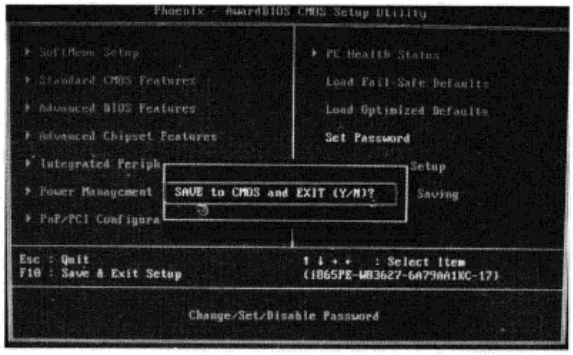


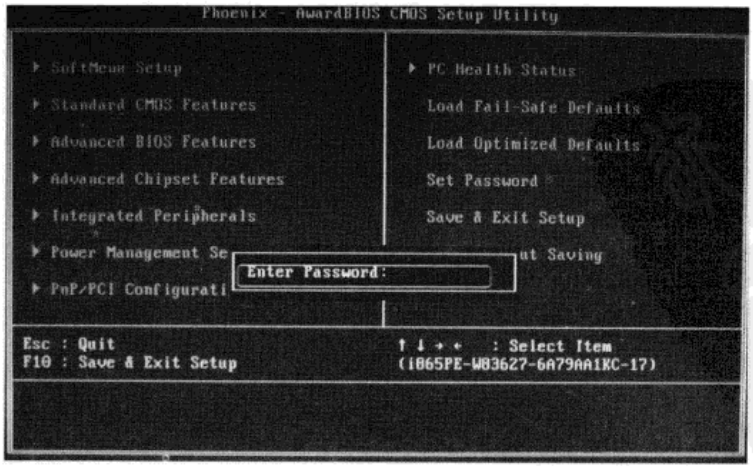

步骤7 系统要求用户再次输入密码确认，在打开的对话框中再次输入密码，输入完成后按下【Enter】键。

步骤8 返回BIOS设置主界面，按下【F10】键，再打开的对话框中输入“y”，然后按下【Enter】键保存设置，稍后计算机会自动重启。




步骤9 计算机重启后，如果想要继续启动计算机或者进入BIOS设置界面就需要输入正确的密码。

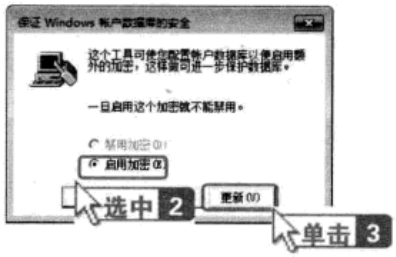


### 2. 设置 Windows 启动密码

对于计算机中保存有重要文件的用户来说，只设置一个CMOS开机密码是不够的，因为一般情况下将主板上的CMOS电池取下放电后，即可将设置的CMOS开机密码清除。CMOS开机密码清除后，使用Active Password Changer软件仍然可以清除管理员账户的登录密码进入操作系统。这时，用户可以设置Windows启动密码。设置Windows启动密码的步骤如下。

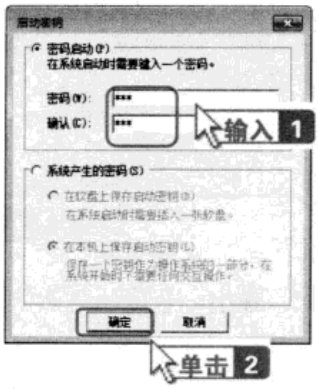
步骤1 在Windows 7系统中选择【开始】➢【运行】菜单项，打开【运行】对话框，在【打开】下拉列表中输入“syskey.exe”，然后按下【Enter】键。

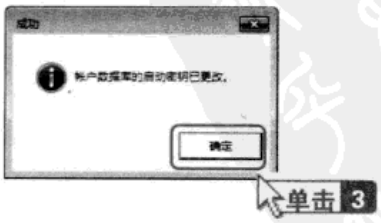
步骤2 打开【保证Windows账户数据库的安全】对话框，选中【启用加密】单选钮，然后单击 更新(U) 按钮。


步骤3 弹出【启动密钥】对话框，在此即可设置Windows的启动密码。选中【密码启动】单选钮，然后在【密码】文本框中输入要设置的密码，在【确认】文本框中再次输入密码进行确认。设置完成后单击 确定 按钮。

步骤4 弹出【成功】对话框，提示账户数据库的启动密钥已更改，然后单击 确定 按钮即可。当用户再次启动计算机时，在进入系统登录界面之前，用户需要输入正确的启动密码才可以进入登录系统。




## 4.1.3 文件加密

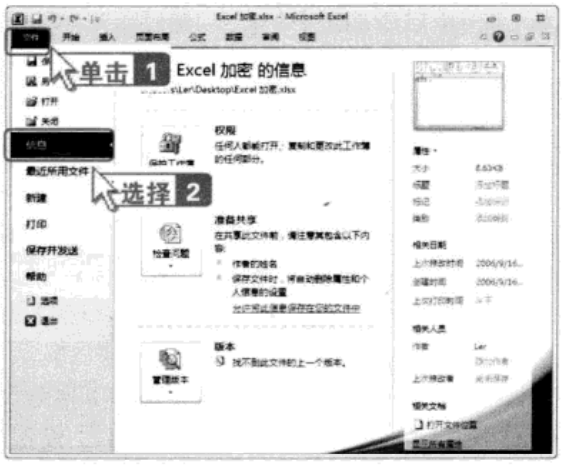
有些时候，电脑是几个人共同使用的，此时为了保护数据的安全，可以给文件加密，这样当其他用户想要使用这些文件就必须输入正确的密码。因此，文件加密对于维护系统的安全起着十

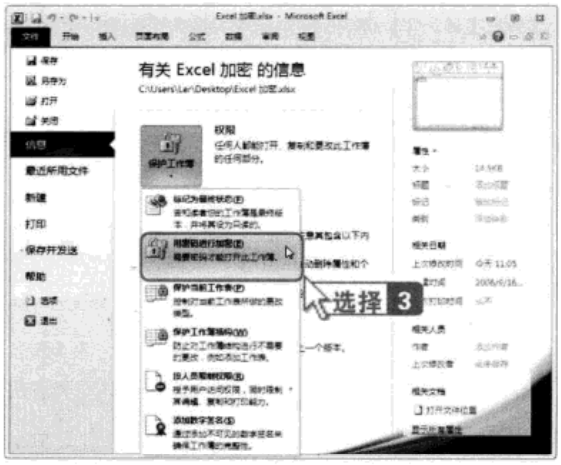
分重要的作用。

Office文档的类型很多，但加密方法都很相似。这里主要介绍如何为Microsoft Office 2010中的Excel文档加密。具体的操作步骤如下。

步骤1 打开要加密的Excel表格，单击【文件】按钮 文件，切换到【文件】选项卡中，在左侧的窗格中选择【信息】选项。

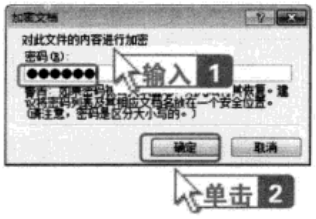
步骤2 在右侧的列表框中单击【保护工作簿】按钮，在弹出的快捷菜单中选择【用密码进行加密】菜单项。

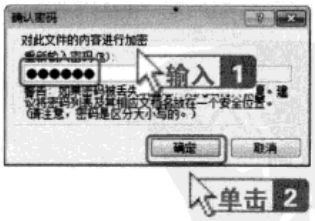



步骤3 弹出【加密文档】对话框，在【密码】文本框中输入加密密码，设置完成后单击 确定 按钮。

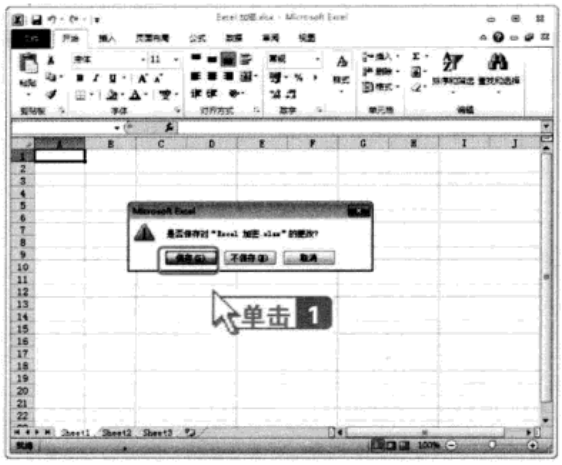
步骤4 弹出【确认密码】对话框，在【重新输入密码】文本框中重新输入一次设置的密码，然后单击 确定 按钮即可。

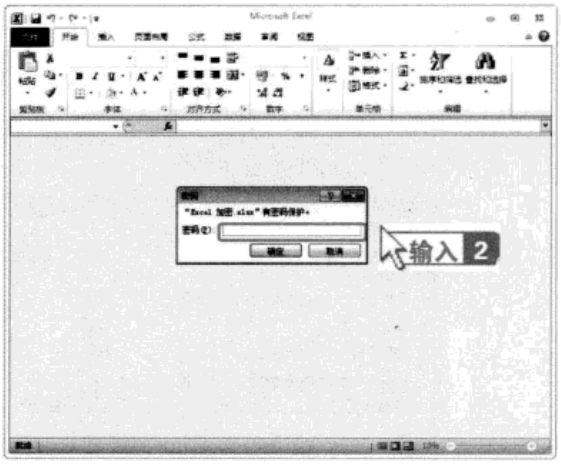



步骤5 设置完成后单击【关闭】按钮关闭该Excel文档，弹出一个提示对话框，提示用户是否保存对该文档的设置，单击 保存(S) 按钮。

步骤6 重新打开该文档，弹出【密码】对话框，用户需要正确输入密码才能够对该文档进行操作。




## 4.1.4 使用加密软件加密

使用加密软件可以实现对文件、文件夹，甚至是应用程序的加密，这样用户可以更加有效地保护自己的私密文件不被非法用户窃取。下面介绍几种常用加密软件的使用方法。

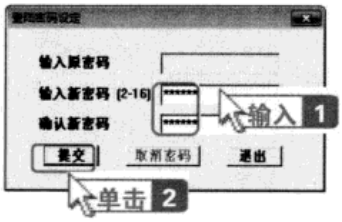
### 1. 使用文件夹加密精灵加密文件夹

文件夹精灵是一款使用方便、安全可靠的文件夹加密软件。它具有安全性高、简单易用、界面美观友好等特点，还具有快速加解密、安全加解密、移动加解密、伪装/还原文件夹、隐藏/恢复文件夹和文件夹粉碎等功能。用户可以使用文件夹加密精灵软件进行私密文件夹的加密，从而保护私密文件。

下面介绍如何使用文件夹加密精灵来加密文件夹，具体的操作步骤如下。

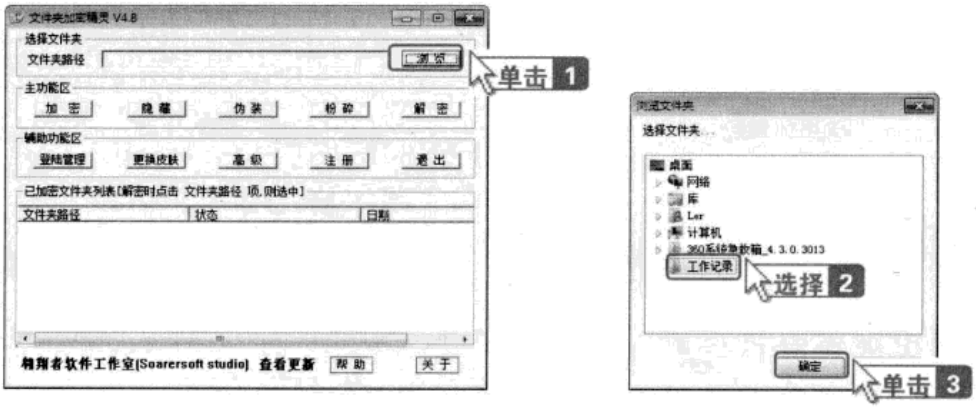
步骤1 安装好“文件夹加密精灵 V4.8”软件后运行该程序，弹出【登录密码设定】对话框，在【输入新密码（2-16）】文本框中输入密码，然后在【确认新密码】文本框中再次输入相同的密码并单击 提交 按钮。这样每次使用文件加密软件都需要输入登录密码。

步骤2 重新运行“文件加密精灵”程序，这时会弹出【文件夹加密精灵登录】对话框，要求用户输入登录密码。在【请输入登陆密码】文本框中输入正确的密码，然后单击 确定 按钮。



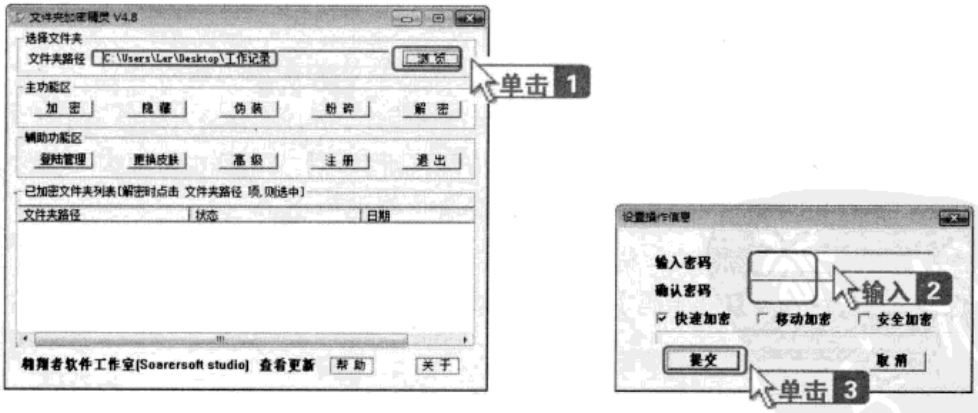

步骤3 进入文件夹加密精灵主界面，在【选择文件夹】组合框中单击 浏 览 按钮。

步骤4 弹出【浏览文件夹】对话框，从中选择想要加密的文件夹的路径，这里选择“工作记录”文件夹，然后单击 确定 按钮。



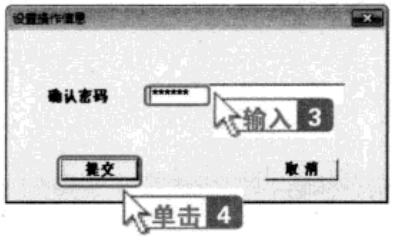

步骤5 返回主界面，可以看到该文件夹路径已经添加到了【文件夹路径】文本框中，接着在【主功能区】组合框中单击 加 密 按钮。

步骤6 弹出【设置操作信息】对话框，在【输入密码】文本框中输入想要设置的密码，然后在【确认密码】文本框中再次输入相同的密码。用户还可以通过选择相应的复选框来选择加密的类型（不同的加密类型具有不同的功能，具体功能可以查看该软件的帮助文档），然后单击 提交 按钮，即可完成该文件夹的密码设置。




步骤7 如果用户想对已经加密的文件夹进行解密操作，那么可以在文件夹加密精灵主界面中的【选择文件夹】组合框中单击 浏 览 按钮，选择需要解密的文件夹，然后单击 解 密 按钮。

步骤8 弹出【操作信息设置】对话框，输入密码并单击 提交 按钮，即可解除已经加密的文件夹的密码。


## 2. 使用金锋文件加密器加密文件

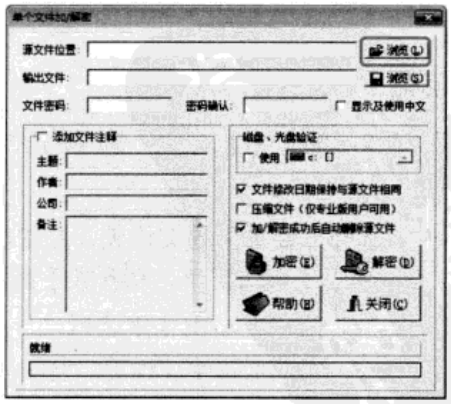
用户除了可以使用文件夹加密软件加密文件夹以外，还可以使用文件加密软件来加密单个或多个文件，从而使文件加密更加细致。

金锋文件加密器集文件加密与压缩、文件夹加密与压缩、文件夹保护、字符串加密、日记本、密码本、文件彻底删除及文件图标提取等功能于一体。用户不仅可以使用该软件中的字符串密码与磁盘、光盘验证等功能对文件和文件夹进行加密，还可以使用它来对文件和文件夹进行压缩，具有较高的压缩率。

下面以“金锋文件加密器 5.5”为例介绍如何使用该软件进行文件的加密。具体的操作步骤如下。

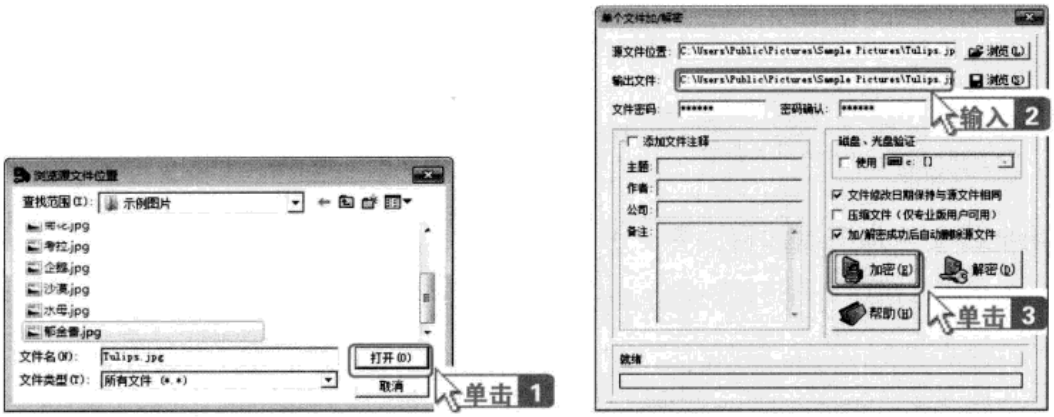
步骤1 安装好“金锋文件加密器 5.5”软件后，运行该程序，打开【金锋文件加密器 5.5】主界面。

步骤2 当用户需要加密单个文件时，可以单击 按钮，弹出【单个文件加/解密】对话框，在【源文件位置】文本框中输入想要加密的文件所在的路径，或者单击 浏览(L) 按钮。

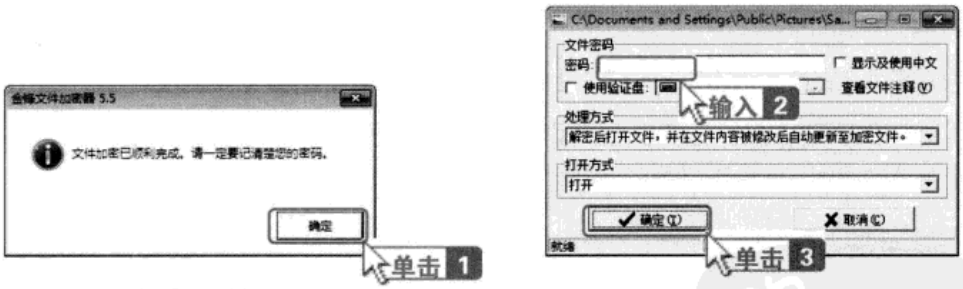
步骤3 弹出【浏览源文件位置】对话框，在该对话框中选择好加密的文件后，单击 打开(O) 按钮。

步骤4 返回【单个文件加/解密】对话框，可以看到该文件的路径自动添加到【源文件位置】文本框中，然后在【输出文件】文本框中输入想要保存的路径（一般选择软件默认的路径）。在【文件密码】文本框中输入想要设置的密码，在【密码确认】文本框中再次输入相同的密码。另外还可以对文件添加注释以及设置磁盘、光盘验证等选项，设置完成后单击 加密(E) 按钮。




步骤5 弹出【金锋文件加密器 5.5】提示对话框，提示用户加密完成，然后单击 确定 按钮即可。

步骤6 当用户打开已经加密的文件时，弹出一个要求用户输入密码的对话框，只有输入正确的密码并单击 ✔确定(O) 按钮后，才能打开该文件。

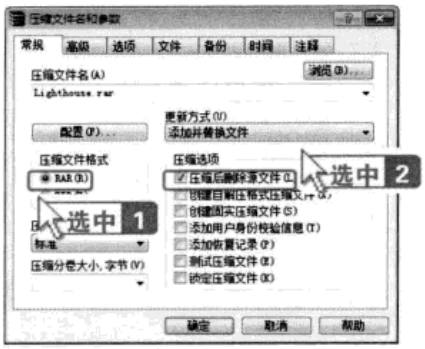



### 3. 使用 WinRAR 加密文件

除了专业的加密软件外，常用的压缩软件WinRAR也可以用来加密文件，具体的操作步骤如下。

步骤1 选择需要加密的文件夹，并单击鼠标右键，在弹出的快捷菜单中选择【添加到压缩文件】菜单项，弹出【压缩文件名和参数】对话框，默认切换到【常规】选项卡，在其中的【压缩文件格式】组合框中选中【RAR】单选钮，并在【压缩选项】组合框中选中【压缩后删除源文件】复选框。

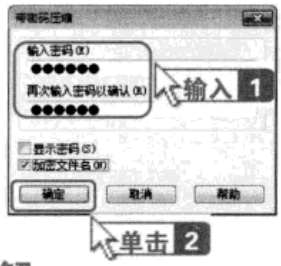
步骤2 切换到【高级】选项卡，单击【分卷】组合框右侧的 设置密码(P)... 按钮。

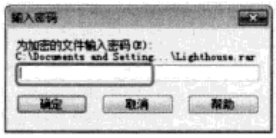




步骤3 弹出【带密码压缩】对话框，在【输入密码】文本框中和【再次输入密码以确认】文本框中输入相同的密码，并选中【加密文件名】复选框，然后单击 确定 按钮。

步骤4 关闭【带密码压缩】对话框，并返回【压缩文件名和参数】对话框，单击 确定 按钮，对文件进行压缩。压缩完成后，重新打开该文件夹的保存窗口，发现“灯塔.jpg”文件消失，出现了一个“Lighthouse.rar”压缩文件。双击此压缩文件，弹出【输入密码】对话框，只有输入正确的密码之后才能打开此压缩文件。



## 4.1.5 密码破解

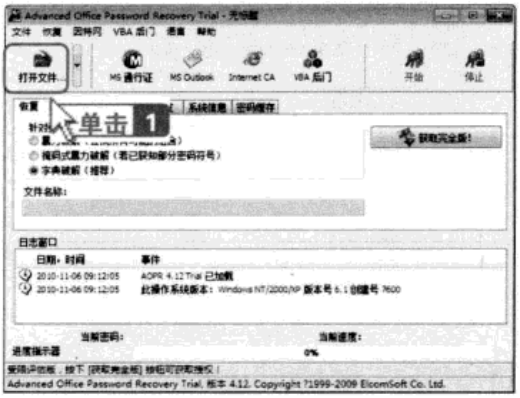
文件加密以后，有时候会忘记密码，此时就需要对文件密码进行破解。

### 1. 破解 Office 文档密码

如果用户忘记了Office文档的密码，可以使用一些相关的密码破解软件进行文档密码的破解。下面就以Advanced Office Password Recovery为例介绍如何使用该软件破解Office文档密码。

步骤1 下载并运行“Advanced Office Password Recovery Professional”程序，打开其主界面，然后单击 按钮。

步骤2 弹出【打开文件】对话框，找到并打开破解的Office文件（这里以“Excel加密.xlsx”为例），然后单击 打开(O) 按钮。





步骤3 打开【预备破解】对话框，进行密码的破解，主界面下方显示了破解的进度。

步骤4 待破解完毕后，打开【Word密码已被恢复】对话框，单击 OK 按钮即可完成该文件密码的破解。

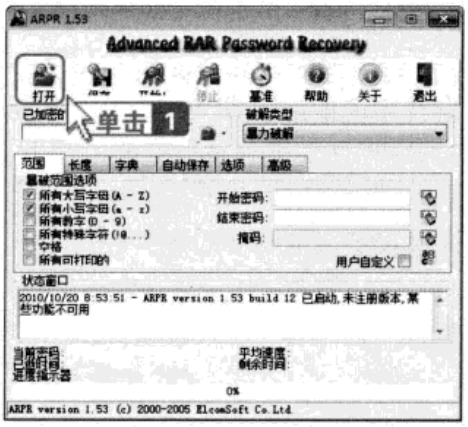
## 2. 破解 WinRAR 文件的密码

WinRAR是一款十分实用的压缩软件，而且它还提供了加密文件的功能，使得用户能够很好地保护自己的文件不被非法用户窃取。

如果用户忘记了设置的WinRAR密码，可以使用一些密码破解软件进行破解，以找回该压缩文件的密码。下面以Advanced RAR Password Recovery为例介绍如何破解WinRAR压缩软件的密码。具体的操作步骤如下。

步骤1 打开【Advanced RAR Password Recovery】主界面，用户可以对密码破解范围（包括长度）进行设置，在工具栏中单击【打开】按钮。

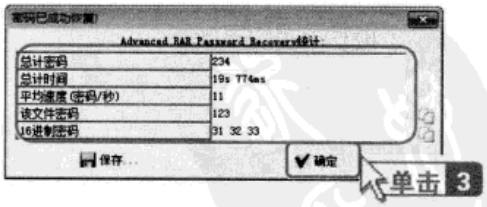
步骤2 弹出【打开】对话框，选择要进行破解的RAR文件，然后单击 打开(O) 按钮。





步骤3 返回主界面，在【破解类型】下拉列表中选择相应的破解类型，在这里选择【暴力破解】选项，并在【暴破范围选项】组合框中选中【所有数字（0-9）】复选框，接着可以切换到【长度】选项卡中，设置需要破解的密码长度，然后单击 开始! 按钮开始密码破解，并在主界面的下面以渐进条显示破解的进度。

步骤4 破解成功后，弹出【密码已成功恢复】对话框，显示破解出的密码，单击 ✔确定 按钮退出该对话框，单击 保存... 按钮可以保存该密码。


## 4.2 远程控制

随着计算机技术的飞速发展，现在很多木马程序并不满足于盗取他人信息，而是开始带有远程控制功能，控制他人的计算机，这样的木马危害更大，防范这样的木马程序也开始受到计算机用户的重视。

### 4.2.1 认识远程控制

所谓远程控制，是指管理人员在异地通过计算机网络异地拨号或双方都接入Internet等手段，

连接被控制的计算机，将被控计算机的桌面环境显示到自己的计算机上，通过本地计算机对远方计算机进行配置、安装程序、修改等工作。

远程控制的工作原理是：远程控制软件一般分客户端程序(Client)和服务器端程序(Server)两部分，通常将客户端程序安装到主控端的电脑上，将服务器端程序安装到被控端的电脑上。使用时客户端程序向被控端电脑中的服务器端程序发出信号，建立一个特殊的远程服务，然后通过这个远程服务，使用各种远程控制功能发送远程控制命令，控制被控端电脑中的各种应用程序运行。

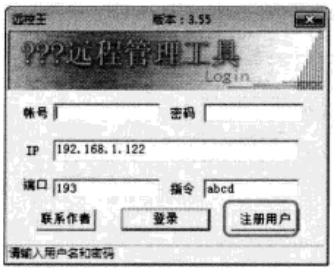
## 4.2.2 使用远程控制软件

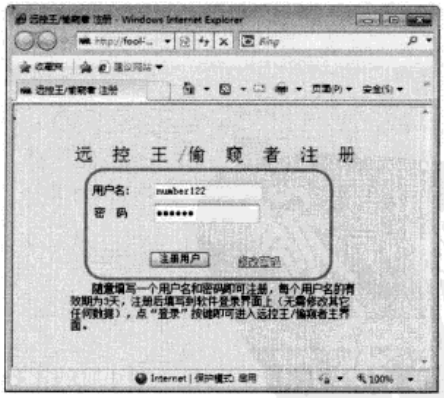
通常所说的控制软件主要指用于正当用途的常规远程控制软件，主要应用包括远程办公、远程教育、远程维护、远程协助等，而黑客常用的远程控制软件却是以病毒复制等形式传播的非法远程控制软件。这些软件通常都是以木马为诱饵，然后让其他用户种上这些木马，进而进行远程操控，这类软件包括远控王、远程控制任我行、灰鸽子远程控制和冰河等，其功能都大同小异。下面介绍如何使用远控王软件来实现远程控制。

远控王是一款常见的木马类远程控制软件，使用该软件进行远程控制的方法很简单。首先进行服务器端配置，具体的操作步骤如下。

步骤1 下载并安装远控王软件，然后运行该软件，打开程序对话框。

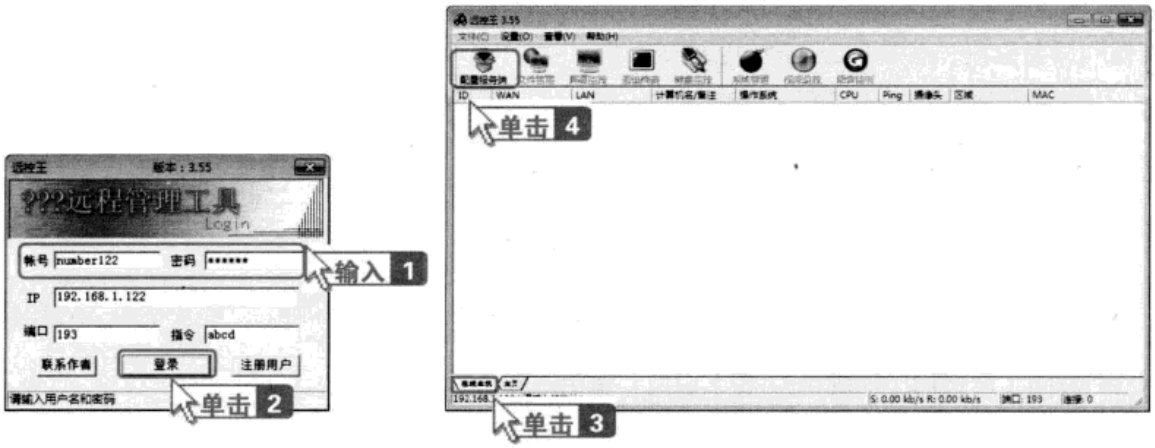
步骤2 如果是第一次使用该软件需要先注册一个账户。单击【远控王】对话框中的 注册用户 按钮，在打开的注册页面中注册一个账户。



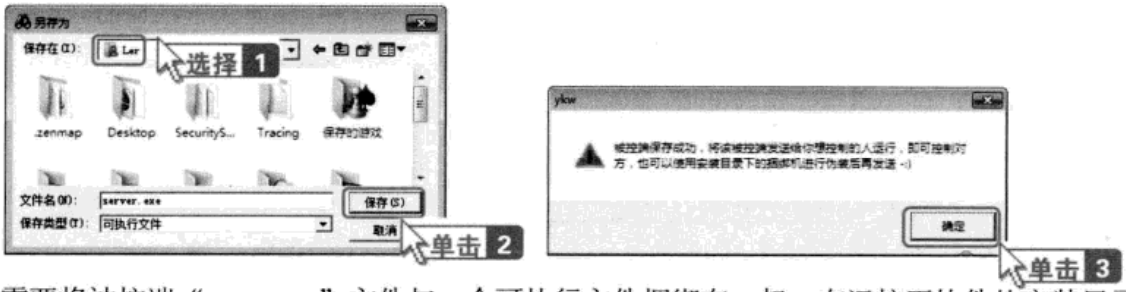

步骤3 注册成功后，在【远控王】对话框中的【账号】和【密码】文本框中分别输入注册的名称和设置的密码，其他采用默认设置，然后单击 登录 按钮。

步骤4 登录成功后会打开远控王主界面，选择远控王主界面底部的【在线主机】选项，切换到在线主机页面中，然后单击页面中的 按钮。




步骤5 弹出【另存为】对话框，为生成的被控端“sever.exe”文件设置保存的位置，设置完成后单击 保存(S) 按钮。

步骤6 弹出【ykw】提示对话框，提示用户被控端生成完毕，单击 确定 按钮即可。

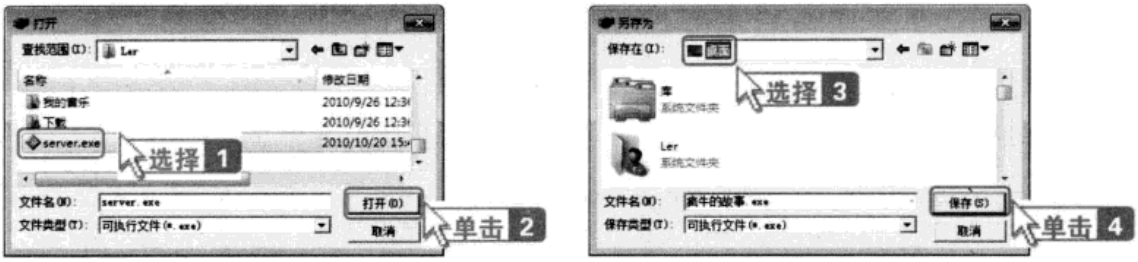



步骤7 需要将被控端“server.exe”文件与一个可执行文件捆绑在一起，在远控王软件的安装目录中找到【捆绑机】文件夹并将其打开，并双击捆绑机程序图标，弹出【傻瓜EXE捆绑机2.0版】窗口，单击 执行文件 1 按钮。

步骤8 在打开的【打开】对话框中找到要捆绑的可执行文件，这里选中远控王软件提供的“疯牛的故事.exe”文件，然后单击 打开(O) 按钮。


步骤9 返回【傻瓜EXE捆绑机2.0版】窗口，接着单击 执行文件 2 按钮，在打开的【打开】对话框中选择生成的被控端文件“server.exe”，然后单击 打开(O) 按钮。

步骤10 返回【傻瓜EXE捆绑机2.0版】窗口，单击 目标文件 按钮，在打开的【另存为】对话框中选择文件的保存位置，然后单击 保存(S) 按钮。




步骤11 返回【傻瓜EXE捆绑机2.0版】窗口，单击 捆绑 按钮。

步骤12 捆绑完成后，弹出【完成】提示对话框，单击 捆绑 按钮，再单击【傻瓜EXE捆绑机2.0版】窗口中的 退出 按钮，返回远控王程序主界面。


至此，服务器的配置完成，接着用户就可以将捆绑生成的程序发给其他人，运行这款程序后，就可以通过服务器端进行远程控制了。

## 4.2.3 防范远程控制

用户的计算机感染了远程控制木马程序后，就有可能被完全控制，这会严重影响用户信息的安全，因此做好必要的防范措施是非常有必要的。

### 1. 木马程序的运作原理

一个完整的木马控制系统主要由控制端、服务端和网络连接三大部分组成，网络连接部分是控制端和服务端建立木马通道的一个重要元素，网络连接一旦中断，便无法实现远程控制。黑客使用远程控制软件实现远程控制大致分为以下几个步骤。

(1) 配置木马服务端程序

配置木马服务端程序是进行远程控制的基础。

(2) 传播木马

黑客在配置好木马服务端程序后，通常会使用各种手段来传播木马程序以实现远程控制。例

如，将木马程序以附件形式通过E-mail发送到用户邮箱中，当收件人打开邮箱中的附件并运行时就可能感染木马程序；另一种最常用的传播方式是通过软件下载，很多不正规的网站通常会将木马程序捆绑在某一个软件安装程序上，然后以提供软件下载的名义引导用户下载，用户下载并运行这些安装程序时，木马程序就会自动安装，木马程序首先将自身复制到系统文件夹中，然后在注册表、启动项等位置设置触发条件，安装完成后便等待与控制端进行连接。

(3) 远程控制

用户的计算机连接网络成功之后，隐藏在用户计算机中的木马程序会自动与控制端进行连接，最终实现远程控制。

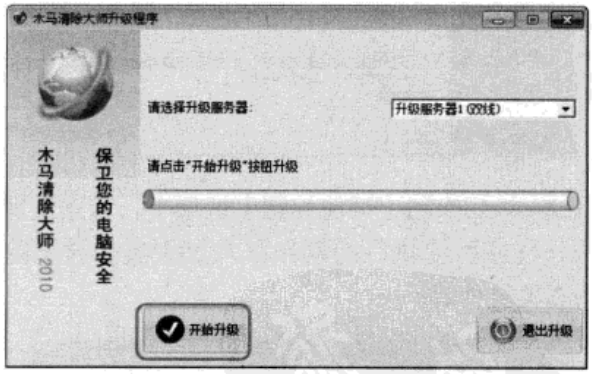
## 2. 防范/查杀木马程序

由于远程木马程序的危害很大，因此做好防范工作是非常必要的。下面介绍一款功能强大的木马查杀工具——木马清除大师。它能够清除210万余种国际国内流行的木马、网络游戏盗号工具、QQ盗密码工具、幽灵后门、流氓软件、间谍软件，查杀率在95%以上。2010版本加强了对系统多种重点区域的检查，可以扫描注册表、Cookies、隐私纪录、服务、敏感区域等，加入了对木马的启发式扫描，木马即使逃脱静态特征码查杀，也无法逃过启发式扫描的“双眼”。

下面介绍如何使用木马清除大师来防御和查杀木马程序。具体的操作步骤如下。

步骤1 从木马清除大师的官方网站上下载并安装最新版的清除软件，安装完成后，运行木马清除大师，打开程序主窗口。

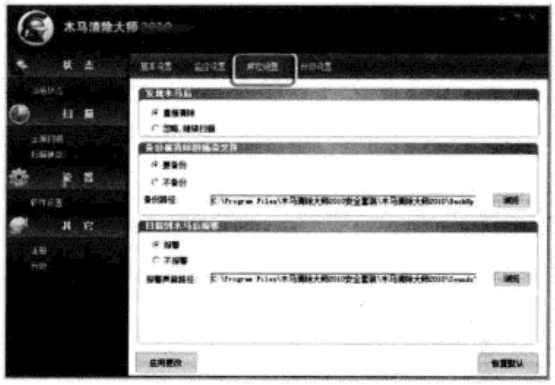

步骤2 如果病毒库过期，一般需要升级病毒库程序，单击主窗口左侧窗格中的【升级】按钮，在打开的升级程序对话框中单击 开始升级 按钮即可升级病毒库。




步骤3 用户在进行全盘扫描之前一般需要设置扫描选项。单击左侧窗格中的【软件设置】按钮，在右侧窗格中即会显示软件设置界面。切换到【基本设置】选项卡，对文件扫描类型、扫描目录等选项进行设置。

步骤4 切换到【监控设置】选项卡，对监控等级和监控规则等选项进行设置。

步骤5 切换到【其他设置】选项卡，设置发现木马程序后要执行的动作以及是否备份被清除的感染文件等。



步骤6 切换到【升级设置】选项卡，对升级模式和升级频率的选项进行设置。

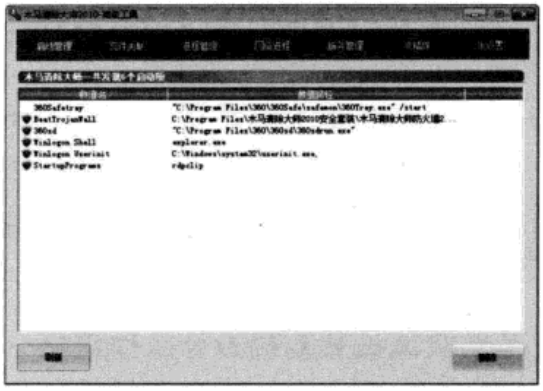
步骤7 设置完成后可进行扫描。如果单击左侧窗格中的【全面扫描】按钮，在右侧的窗格中对要扫描的内容进行选择，然后单击 按钮。

步骤8 扫描完成后，在右侧的【扫描结果】组合框中可以看到扫描的结果，单击 按钮。

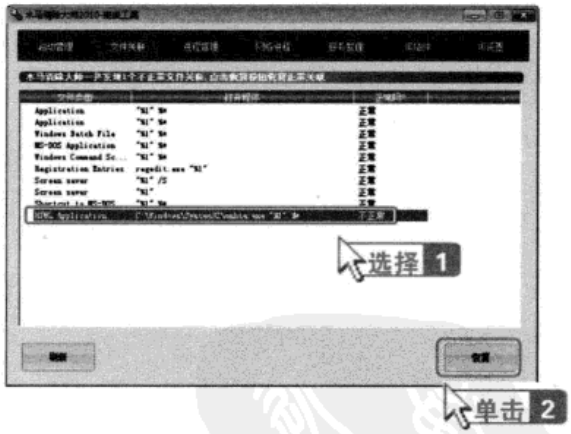
步骤9 在弹出的对话框中会显示详细的扫描信息。单击扫描结果中列出的某个有害项目，在右侧的【帮助信息】组合框中会显示出相应的描述信息。如果想要清除所有的有害项目，则单击对话框中的 按钮即可将其删除。

步骤10 如果要对磁盘分区进行扫描，则在程序的左侧窗格中单击【扫描硬盘】按钮，在右侧的窗格中选中要扫描的磁盘分区，然后单击 按钮即可进行自定义扫描。

步骤11 用户还可以单击左侧窗格中的【当前状态】按钮，在右侧的窗格中单击【工具列表】组合框中的【系统诊断工具】超链接，打开【木马清除大师-高级工具】窗口，其中包含七大功能，可以轻松查杀各种恶意软件，是用户诊断系统的有力助手。



步骤12 在【木马清除大师-高级工具】窗口中可以对启动项、文件关联、活动进程、网络进程和系统服务等项目进行设置。如果系统中存在不正常的文件关联，切换到【文件关联】选项卡，选中不正常的文件关联选项，然后单击 按钮即可恢复为正常关联。



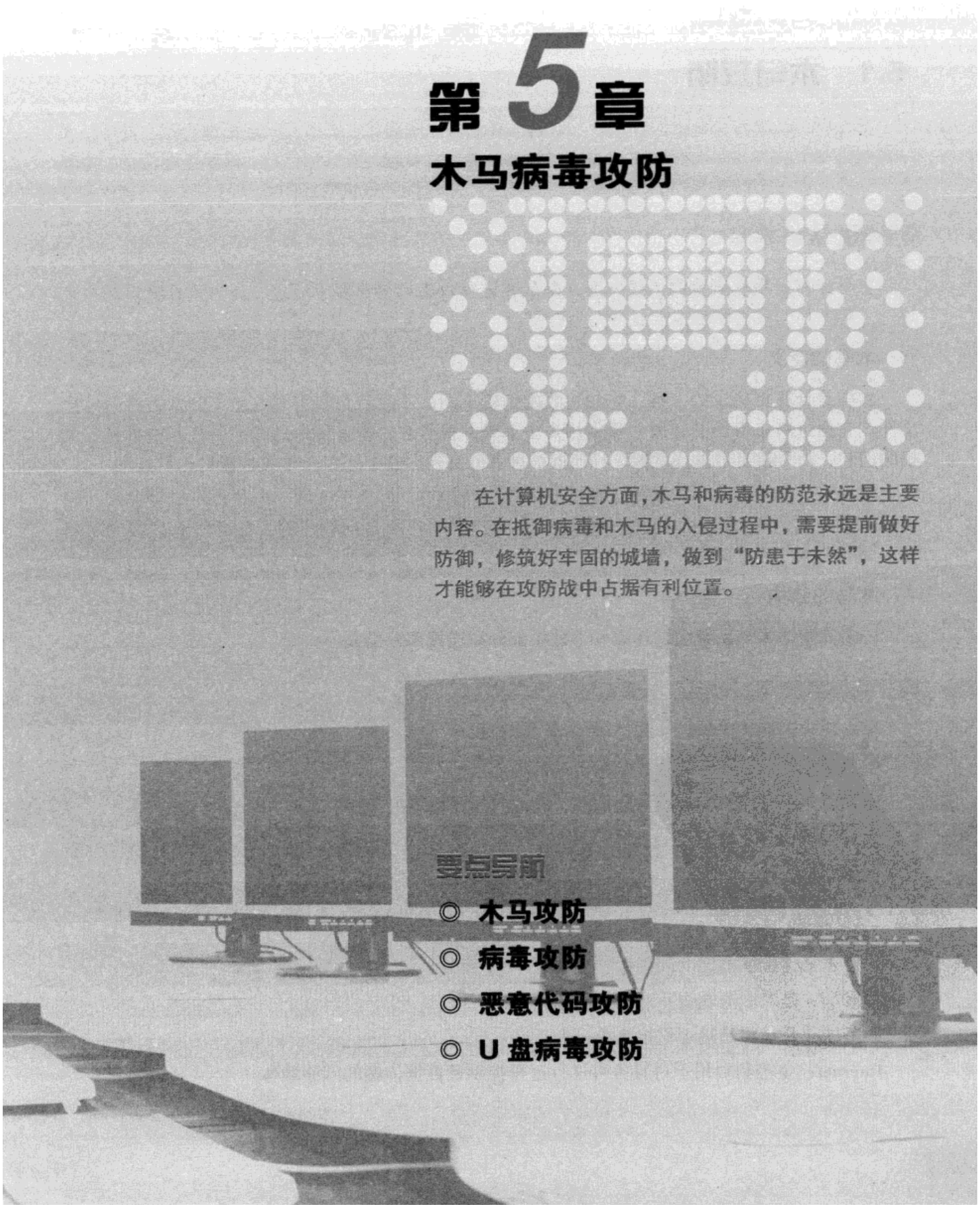
## 新手问题解答

### 如何为自己的主机设置一个 CMOS 密码

计算机在启动时首先要进行CMOS自检，然后才会进入操作系统，用户可以参照4.1.2的内容为自己的主机设置一个CMOS密码，这样在计算机启动时，用户必须输入CMOS密码才能够继续计算机的启动。

### 为防火墙设置密码有什么作用吗

目前流行的防火墙中，有些防火墙有设置密码功能，用户通过为自己的防火墙设置密码，为防火墙的操作设置增加安全保障，从而有效地阻止他人篡改自己对防火墙的设置。



# 第5章 木马病毒攻防

在计算机安全方面，木马和病毒的防范永远是主要内容。在抵御病毒和木马的入侵过程中，需要提前做好防御，修筑好牢固的城墙，做到“防患于未然”，这样才能够在攻防战中占据有利位置。

## 要点导航

- ◎ 木马攻防
- ◎ 病毒攻防
- ◎ 恶意代码攻防
- ◎ U盘病毒攻防

# 5.1 木马攻防

木马攻击是黑客最喜爱的攻击手段，利用其他的一些载体，木马可以轻松地隐藏在其中。木马的危害在于它对计算机有着强大的控制和破坏能力，同时还有窃取密码、偷窥重要信息、控制系统操作、进行文件操作等能力，从而达到完全控制目标计算机的目的。

## 5.1.1 认识木马

木马一直是黑客研究的主要内容，是黑客进行攻击的最重要手段之一。对于计算机用户来说，了解木马的攻击原理也就显得尤为重要。

### 1. 木马的定义

木马是计算机病毒的一种，它与一般的病毒不同，不进行自我繁殖，也不刻意去感染其他文件，它通过将自身伪装起来，吸引用户去下载并执行它，向种植木马者提供打开被种者计算机的门户，使种植者可以任意毁坏和窃取被种者的文件，甚至远程操作被种者的计算机。

木马与计算机网络中常用的远程控制软件有些相似，但由于远程控制软件是直接控制，因此通常不具有隐蔽性；木马则完全相反，它要达到的目的是远程控制，如果没有很强的隐蔽性，那就没有任何意义了。

### 2. 木马的结构

一个完整的木马系统由软件部分、硬件部分和连接部分组成。

#### ○ 软件部分

实现远程控制也需要软件程序的支持，软件程序主要包括以下3个方面。

控制端程序：是用于远程控制服务端的程序。

木马程序：是用于潜入服务端内部，获取其操作权限的程序。

木马配置程序：是用于设置木马程序的端口号、触发条件及木马名称等，使其在服务端藏得更隐蔽的程序。

#### ○ 硬件部分

建立木马连接所需要的硬件主要包括以下3个部分。

控制端：是对服务端进行远程控制的一方。

服务端：是被控制端远程控制的一方。

Internet：是控制端用于对服务端进行远程控制及数据传输的网络载体。

### 连接部分

连接部分是通过Internet在服务端和控制端之间建立一条木马通道所必需的条件。

控制端IP/服务端IP：即控制端/服务端的网络地址，也是木马进行数据传输的目的地。

控制端端口/木马端口：即控制端/服务端的数据入口。通过这个入口，数据可直达控制端程序或木马程序。

## 3. 木马的特征

自从木马出现以来，到现在已经出现了很多种类，但所有木马都具有以下几个基本的特征。

### 隐蔽性

木马也是一种病毒，它必须隐藏在用户的系统之中并想尽一切办法不让用户发现。一般的局域网间通信软件在运行时，客户端与服务器端连接成功之后客户端上会出现很醒目的提示标志。而木马类的软件的服务器端在运行时会应用各种手段隐藏自己，不会提示，因为设计者不会低级到让用户轻易地发现木马。例如，修改注册表和配置文件使计算机在下一次启动之后能自动载入该木马程序，它并不是自身生成一个启动程序，而是依附在其他的程序中。

木马的隐蔽性主要表现在两个方面：一是不产生图标；二是木马程序会自动隐藏在任务管理器中，并以系统服务的方式欺骗操作系统来攻击用户。

### 自动运行

木马是在用户系统启动时自动运行的程序，因此木马必须潜入计算机的启动配置文件中，如win.ini、System.ini、Winstart.bat以及启动项等文件之中。

### 欺骗性

木马程序要达到长期隐蔽的目的，就必须借助系统中已有的文件，以防被用户发现。它一般使用常见的文件名或扩展名，或者仿制一些不易被人区分的文件名，甚至直接借用系统文件中已有的文件名，只不过它保存在不同的路径中。有的木马程序会将自己设置成一个IE图标，当用户不小心打开它就会马上运行。

### 自动恢复性

现在很多木马程序中的功能模块已不再是由单一的文件组成，而是具有多重备份、可以相互恢复的，这就大大增大了删除的难度。

### 功能特殊性

木马的功能通常都比较特殊，除了普通的文件操作外，还有一些木马具有搜索Cache（缓存）中的口令、进行键盘记录、设置口令、扫描目标计算机的IP地址、远程操作注册表以及锁定鼠标等功能。这与正当的远程控制软件是不同的，正当的控制软件是为了方便管理员的操作和管理，而不是攻击对方的计算机。

## 5.1.2 木马的分类

木马程序自出现至今已经出现了各种各样的类型，绝大多数的木马并不是只具有单一功能，而是很多种功能的集成品，甚至有很多技术超一流的功能在一些木马中广泛存在。

### 1. 远程木马

远程木马也叫远程控制木马，它是数量最多、危害最大，同时知名度也是最高的一种木马，它可以让攻击者完全控制被感染的计算机，攻击者可以利用它完成一些甚至是计算机管理员都不能轻易完成的操作，其危害之大不言而喻。由于要到达远程控制的目的，该类木马往往拥有其他种类木马的一些功能，使其在被感染的计算机上能随便操作，可以任意访问文件，甚至监视对方在计算机上的一举一动。

国产木马“冰河”就是一个远程访问型特洛伊木马，这类木马使用起来非常简单，只需运行服务端并得到受害人的IP，黑客即可访问。远程访问型木马的普通特征是键盘记录、上传和下载、注册表操作、限制系统功能及判断系统信息等。远程访问型特洛伊木马会在用户的计算机打开一个端口以保持连接。

### 2. 键盘木马

键盘木马功能简单，它只做一件事情，就是记录受害者的键盘敲击并在日志文件里查找密码。这种特洛伊木马随着Windows的启动而启动，一般有在线和离线记录这样的选项，也就是说用户在线和离线状态下敲击键盘都会被植入木马的幕后黑客获取，黑客从这些按键中以特殊的方法得到用户的密码等有用的信息。当然，对于这种类型的木马，邮件发送功能也是必不可少的。

### 3. 密码发送型木马

现今社会信息安全日益重要，密码则是通向重要信息的一把极其有用的钥匙，只要掌握了对方的密码，从很大程度上就可以轻而易举地得到对方的很多信息，而密码发送型木马正是专门为了盗取被感染的计算机上的密码而编写的。该木马一旦被执行，就会自动搜索内存、Cache、临时文件夹以及各种敏感的密码文件，一旦搜索到有用的密码，木马就会利用免费的电子邮件服务将密码发送到指定的邮箱，从而达到获取密码的目的，因此这类木马大多使用25号

端口发送E-mail。大多数的密码发送型木马不会在每次系统重启的时候重启。这种木马的目的是找到所有的隐藏密码并且在受害者不知道的情况下把它们发送到指定的邮箱。

由于黑客需要获得的密码多种多样，用户计算机上密码的存放形式也大不相同，所以很多时候黑客都需要主机编写程序，从而得到符合自己要求的木马。

### 4. 破坏型木马

破坏型木马唯一的功能就是破坏被感染计算机的文件系统，使其遭受系统崩溃或者重要数据丢失的巨大损失。从这一方面上来说，它和病毒很类似。不过这种木马的激活是由攻击者控制的，并且传播能力也弱于病毒。

### 5. Dos 木马

随着Dos攻击越来越被黑客广泛应用，被用做DoS攻击的木马也越来越流行。当黑客侵入一台计算机并种上了DoS攻击木马，那么日后这台计算机就成了黑客DoS攻击最得力的帮手。黑客控制的计算机数量越多，发动DoS攻击取得成功的概率就越大，所以这种木马的危害不是体现在被感染的计算机上，而是体现在攻击者可以利用它来攻击网络上其他的计算机，给网络造成很大的危害和损失。

还有一种类似DoS的木马叫做邮件炸弹木马，机器一旦被该木马感染，就会随机生成各种各样主题的信件，对黑客指定的邮箱不停地发送邮件，一直到对方邮箱瘫痪而不能接收邮件为止。

### 6. FTP 木马

FTP木马可能是最简单和古老的木马了，该木马唯一的功能就是打开21端口，等待用户连接。现在新型FTP木马还加上了密码功能，这样，只有攻击者本人才知道正确的密码，从而顺利地进出对方的计算机。

### 7. 代理木马

黑客在入侵时往往掩盖自己的足迹，谨防别人发现，通过代理木马，攻击者可以在匿名的情况下使用Telnet、IRC等程序，从而隐蔽自己的踪迹。给被控制的计算机种上代理木马，让其变成攻击者发动攻击的跳板就是代理木马最重要的任务。

### 8. 程序禁用木马

常见的防木马软件有瑞星、Norton Anti-Virus及木马清除大师等。程序禁用木马的功能就是关闭对方计算机上运行的这类程序，以便让其他的木马更好地发挥作用。

### 9. 反弹端口型木马

防火墙对于连入的链接往往会进行非常严格的过滤，但对于连出的链接却往往疏于防范。

于是与一般的木马相反，反弹端口型木马的服务端（被控制端）使用主动端口，客户端（控制端）使用被动端口。木马定时监测控制端的存在，一旦发现控制端上线，立即弹出端口，主动连接控制端打开的主动端口；为了隐蔽起见，控制端的被动端口一般设置在80端口（浏览网页必开端口）上，这样即使用户使用端口扫描软件检查自己的端口，发现的也是类似“TCP UserIP:3688 ControllerIP:80ESTABLISHED”的情况，不明真相的用户就会以为是自己在浏览网页，并且防火墙也会这么认为，因为防火墙一般不会禁止用户向外连接80端口。

### 5.1.3 常见的木马入侵和伪装手段

木马程序为了达到目的，会入侵用户的计算机，为了不被用户发现，会使用一些伪装手段。

#### 1. 常见的木马入侵手段

木马程序虽然多种多样，但大多数没有什么特别的功能，其入侵的方法也很相似，只是将以前的木马程序更换了名称而已。下面介绍一些木马通用的入侵手法。

##### ● 在 win.ini 中加载

一般在win.ini文件中的Windows中有加载项“run=”和“load=”，此两项通常为空。如果发现这两项加载了任何可疑的程序时需要特别当心，这时可以根据其提供的源文件路径和功能进一步检查。这两项分别用来自动运行和加载程序，如果木马程序加载到这两个子项中后，那么系统启动后即可自动运行或者加载。当然也有可能系统中确实需要加载某一程序，但这更是木马利用的好机会，它往往会在现有加载的程序文件名之后再加一个它自己的文件名或者参数，该文件名一般使用用户常见的command.exe、sys.com等文件来伪装。

##### ● 在 system.ini 文件中加载

在系统信息文件system.ini中也有一个启动加载项，那就是在【BOOT】子项中的“Shell”项。在这里木马最惯用的伎俩就是把本应是“Explorer”变成它自己的程序名，这些改变如果不仔细留意是很难发现的，这就是前面所讲的欺骗性。当然也有的木马直接把“Explorer”改为别的什么名字，或者在“Explorer”加上一个不显眼的木马程序。

##### ● 在 Winstart.bat 中启动

Winstart.bat是一个特殊性丝毫不亚于Autoexec.bat的批处理文件，也是一个能自动被Windows加载运行的文件。它多数情况下为应用程序及Windows自动生成，在执行了Win.com并加载了多数驱动程序之后开始执行。由于Autoexec.bat的功能可以由Winstart.bat代替完成，因此木马完全可以像在Autoexec.bat中那样被加载运行，危险即由此而来。

### 在启动项中加载

木马隐藏在启动组中虽然不是十分隐蔽，但这里的确是自动加载运行的好场所，其最大的优势是只要用户启动计算机，木马就会自动运行，因此还是有木马驻留在这里。启动在注册表中的位置是HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run。当用户打开【Run】选项时，发现注册表中多了很多可疑的启动项，这就说明用户极有可能已经中木马了。

### 利用*.INI 文件

*.INI文件即应用程序的启动配置文件。控制端利用这些文件能启动程序的特点，将制作好的带有木马启动命令的同名文件上传到服务端覆盖同名文件，这样就可以达到启动木马的目的了。

### 修改文件关联

修改文件关联是木马常用的手段，正常情况下txt文件的打开方式为用notepad.exe文件。但中了文件关联木马之后，txt文件的打开方式就会被修改为用木马程序打开，例如，著名的冰河木马采用的就是这样的方式。一旦用户双击一个txt文件，原本应该用notepad.exe打开该文件，现在却变成启动木马程序了。不仅仅是txt文件，其他的诸如HTM、EXE、ZIP、COM等都是木马的目标。要对付这类木马，只能检查HKEY_CLASSES_ROOT项下相关文件类型的后缀名（\shell\open\command主键），查看其键值是否正常。

### 捆绑文件

实现捆绑文件的触发条件是首先需要控制端和服务端已通过木马建立连接，然后控制端用户使用工具软件将木马文件和某一应用程序捆绑在一起，随即上传到服务端覆盖原文件。这样即使木马被删除了，只要运行捆绑木马的应用程序，木马又会被重新安装，绑定到某一应用程序中。如果绑定到系统文件，那么每一次启动Windows时均会同时启动木马。

## 2. 揭露木马的伪装手段

随着木马技术被越来越多的计算机用户所了解，防范意识增强，木马的传播也遇到了一定的困难。木马的设计者为了能够更好地降低用户的警惕心，达到欺骗用户的目的，常常设计一些特殊的手段来对木马进行伪装。

### 修改图标

木马服务端所用的图标有一定的规律可循，木马经常故意伪装成XT.HTML，等待用户由于疏忽而将其认为是没有危害的文件图标而将其打开。

### 捆绑文件

这种伪装手段是将木马捆绑到一个安装程序中，当安装程序运行时，木马就会在用户毫无觉察的情况下偷偷地进入系统。被捆绑的文件一般是可执行文件，如EXE、COM等文件。

### 出错显示

有一定木马知识的人都知道，如果打开一个可执行文件却没有任何反应，这很可能是一个木马程序。木马的设计者也意识到了这个缺陷，所以有的木马提供了一个叫做出错显示的功能。当服务器用户打开木马程序时，就会弹出一个错误提示框（这当然是谎报的），错误内容可自由定义，如“文件已破坏，无法打开！”之类的信息，当服务端用户信以为真的时候，木马已经悄悄侵入了系统。

### 定制端口

很多老式的木马端口都是固定的，这给判断是否感染了木马带来了方便，只要查一下特定的端口就知道感染了什么木马。因此现在很多木马都加入了定制端口的功能，控制端用户可以在1024~65535之间任选一个端口作为木马端口（一般不选1024以下的端口），这样就给判断所感染的木马类型带来了麻烦。

### 木马更名

如果木马的名称不做任何修改，那么用户通常能够很容易地辨认出木马程序。为了增强木马的欺骗性，木马设计者经常给木马取一个具有迷惑性的名称，或者允许控制端用户自由定制安装后的木马文件名，这样就很难判断所感染的木马类型了。木马大多数是改为与系统文件名类似的名称，例如，有的木马将名称改为window.exe，或者把.dll改为.dl等。

### 扩展名欺骗

这是许多黑客惯用的一个欺骗方法，就是将木马伪装成图像、文档等文件，这一点与木马更名的性质相似，但这一招看上去虽然很不合逻辑，却有许多用户中招。

例如，图像文件的扩展名根本就不可能是exe，而木马程序的扩展名基本上又必定是exe，这样，多数用户在看到扩展名为exe的文件时就会很小心。于是木马设计者就将文件名进行一些改变，例如将“photo.exe”更改为“photo.jpg.exe”，因为Windows默认是不显示扩展名的，于是用户只能看见一个“photo.jpg”文件了。此时如果用户的计算机恰好是设定为隐藏扩展名的话，就很容易将其当成一个图片而启动了。

选择【开始】➢【控制面板】菜单项打开【控制面板】窗口，双击【文件夹选项】图标，打开【文件夹选项】对话框并切换到【查看】选项卡，取消选中【高级设置】组合框中的【隐藏已知文件类型的扩展名】复选框，然后单击 确定 按钮，这样所有系统已知的文件就会显示其完整的扩展名了。

### 自我销毁

自我销毁功能是为了弥补木马的一个缺陷而设计的。当服务端用户打开含有木马的文件后，木马会自动拷贝到Windows系统文件夹中（C:\wmdows或者C:\windows\system目录下）。一般来说，源木马文件和系统文件夹中的木马文件大小是一样的（捆绑文件的木马除外），那么用户只要在近来收到的邮件和下载的软件中找到源木马文件，然后根据源木马的大小去系统文件夹中找相同大小的文件，判断哪一个是木马即可。木马的自我销毁功能是指安装完木马之后，源木马文件会自动销毁，这样服务端用户就很难再找到木马的来源了，此时在没有查杀木马工具的帮助下是很难删除木马的。

## 5.1.4 木马诊断

在病毒猖獗的网络上，木马这一类病毒是流传最为广泛的，黑客用它来盗取用户信息，获得非法利益，那么如何判断自己的计算机是否被木马控制了呢？下面介绍被木马控制的计算机的一些表现。

### 1. 计算机中木马的表现

黑客可以通过木马盗取用户信息，获得非法利益，或是通过木马控制用户计算机，进行网络攻击。计算机中木马后通常会有以下几种表现。

### 聊天工具的异常登录提醒

聊天工具的异常登录提醒是指用户登录聊天工具时，聊天工具弹出的登录提醒。例如，用户登录QQ时，QQ会提示用户上一次登录的地点，如果用户上一次没有在提示地点登录，那么一定是QQ账号和密码泄露，这就说明计算机很有可能中了木马，黑客通过木马取得了用户的QQ账户和密码，从而在其他地方登录。当然也有可能是以其他方式泄露的。此时用户应该使用杀毒软件查杀，以确保计算机的安全。

### 网络游戏登录不正常

登录网络游戏时发现装备丢失或者和上次下线时的位置不符，甚至使用正确的密码无法登录。如果用户没有通过其他途径泄露过自己的游戏账号和密码，那么就一定是被计算机上的木马程序泄露了，此时用户也应该查杀木马，以防止信息继续泄露。

### 用户突然失去了计算机的控制权

用户在使用计算机过程中，突然发现鼠标在用户不动的情况下自己在动，并且还会单击有关的按钮进行操作，此时可能是有人通过木马在远程控制用户的计算机，用户应该立即断开网络，使用杀毒软件查杀木马。

### 硬盘读写不正常

硬盘读写不正常是指用户在没有读写硬盘的情况下，硬盘灯却指示为硬盘正在读写( 也就是硬盘灯不停地闪烁 )，此时很有可能是有人通过木马在复制用户计算机上的文件。在大量读写文件时，系统还会变慢，此时用户应立即拔掉网线，检查系统进程是否正常，并使用工具进行查杀。

### 摄像头被非正常使用

当用户准备使用摄像头时，系统提示“该设备正在使用”，说明攻击者已经在盗用用户的摄像头了。这种情况下，摄像头的工作状态是不可见的。建议用户在不用摄像头时，把镜头盖上，这样攻击者看到的就是黑糊糊的影像。

### 网络连接异常活跃

在用户没有使用网络资源时，发现网卡灯在不停闪烁。一般来说，在用户没有使用网络资源时，网卡灯会比较缓慢地闪烁，如果此时网卡灯不停闪烁，十分活跃，说明有软件在用户不知道的情况下连接网络，该软件一般是木马程序，正常的软件是不会在用户不知情的情况下连接网络的。

一般来说，计算机中了木马的表现主要有以上几点，但并不是说没有上述表现的计算机就一定是安全的，要想保证计算机的安全，用户还需按时使用杀毒软件进行查杀。

## 2. 计算机中木马的途径

和其他的病毒一样，计算机中了木马也是通过一定途径的，不可能无缘无故的计算机就中了木马，木马传播的途径主要有以下两种。

### 浏览了带有木马的网站

现在很多黑客在一些网站上挂了木马，如果用户在不知情的情况下浏览了这些网站，那么用户的计算机很有可能感染木马。要预防这种情况，用户就需要注意不要浏览一些不健康的网站，另外要开启杀毒软件的主动防御功能。

### 通过聊天工具接收了带有木马的文件

有很多黑客常常会将木马捆绑在正常文件中，然后将该文件通过聊天工具传递给用户，用户只要运行该文件就会中木马。要预防这种情况，用户就要注意不要接收陌生人传送的文件，同时，接收的文件一定要用杀毒软件查杀后再使用。

## 3. 木马的防范策略

反木马就像反病毒一样是永远没有止境的，也永远没有一个万能的解决方案，因为都是先有木马，然后才有反木马的软件，计算机用户始终是一个追随者。所以最好的对付木马的方法就是防止其入侵，防患于未然。下面介绍防范木马的几个方面，经常注意这些方面就可以大大降低被木马攻击的概率。

### 谨慎对待任何来历不明的软件

在安装和使用从网上下载的软件之前一定要用反病毒软件，最好是专门查杀木马的软件进行检查，确定里面没有病毒和木马之后再安装和使用。

### 不要轻信他人

不要随意运行他人发送来的软件。网络发展到今天，谁都不能保证发来邮件或软件的人一定是自己的朋友，因为别人也可以冒名大肆地发送邮件；其次虽然明知对方并无恶意，但也不能确保对方的计算机上就不会有病毒，也许对方的计算机已经中了黑客程序而自己还不知道，这样病毒和木马就会随之传播。

### 不要随便下载软件

不要随便从网站上下载软件，特别是不可靠的小FTP站点、公开新闻组和BBS论坛，因为这些地方正是新病毒和木马发布的首选之地。

### 不要随便留下自己的个人资料

不要随便留下自己的个人信息，特别不要在聊天室内公开自己的E-mail地址。因为黑客攻击的第一步就是处心积虑地搜集网络上的一切资料，在网络上公开的一切资料都有可能成为黑

客的垫脚石。更不要将重要口令和资料存放在连接到Internet的计算机中，以防黑客侵入计算机获取这些信息。

### 谨慎使用自己的邮箱

谨慎使用自己的邮箱，即使是从未公开过的安全性非常高的邮箱或者ISP邮箱，并且用户已经设置了过滤系统，也不能保证能够百分百地拒绝垃圾邮件、病毒和木马。

### 最好使用第三方邮件程序

最好使用第三方邮件程序，如Foxmail等，不要使用Microsoft的Outlook程序。因为Outlook程序的安全漏洞实在是太多了，而且Outlook也是黑客首选攻击的对象。

### 始终显示 Windows 文件的扩展名

使用前面介绍的方法进行设置，总是显示Windows文件的扩展名。不过此时需要防止黑客实施扩展名欺骗攻击，一般来说，扩展名为VBS、SHS或PIF的文件多为木马病毒的特征文件。

### 运行反木马实时监控程序

在上网时一定要运行反木马实时监控程序、专业的最新杀毒软件和个人防火墙等进行监控。

### 给电子邮件加密

为了确保自己的邮件不被其他人看到，同时也为了防范黑客的攻击，可以使用PGP等加密软件给电子邮件加密。

### 隐藏 IP 地址

在上网时最好用一些工具软件隐藏自己计算机的IP地址，这一点非常重要。

### 不要轻易打开不明附件的链接

广告邮件中的附件或其中的链接都是木马程序依附的重要对象。

### 尽量少用共享文件夹

如果需要共享文件，最好单独设置一个共享文件夹，把所有需要的文件都放在该共享文件夹中，一定不要将系统目录设置为共享文件夹。

## 5.1.5 木马制作与防范

通常情况下，木马都是隐藏在一些文件中，所以木马的制作就会依赖文件。下面介绍软件捆绑木马、自解压木马、Chm电子书木马的制作方法与防范。

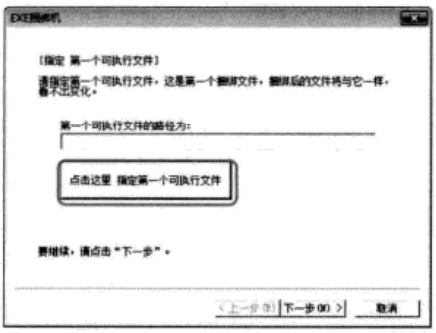
### 1. 软件捆绑木马

软件捆绑木马的制作通常依靠软件，这样的软件很多，操作起来也很方便。

#### 捆绑木马的制作

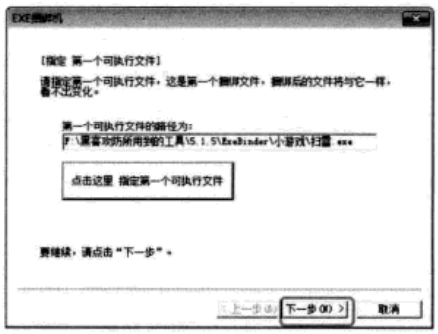
捆绑木马的软件很多，这里以利用“EXE捆绑机”软件进行木马捆绑为例进行介绍，具体的操作步骤如下。

步骤1 下载“EXE捆绑机”软件，并双击运行该软件，打开【EXE捆绑机】对话框，然后单击 点击这里 指定第一个可执行文件 按钮。

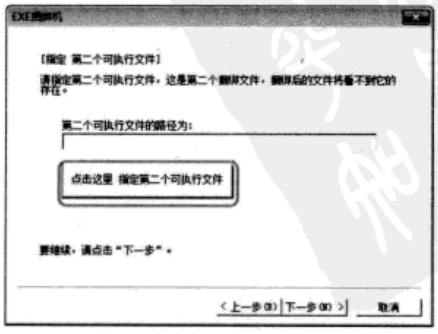



步骤2 打开【请指定第一个可执行文件】对话框，选中一个该软件自带的EXE文件，这里选中“扫雷.exe”小游戏，然后单击 打开(O) 按钮。


步骤3 返回【指定 第一个可执行文件】对话框，此时可以看到刚刚选中的EXE文件路径已经添加进来了，然后单击 下一步(N) > 按钮。

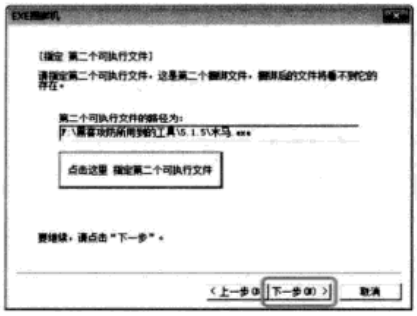



步骤4 弹出【指定 第二个可执行文件】对话框，并单击 点击这里 指定第二个可执行文件 按钮。这里面也需要添加一个.exe文件，而且捆绑后看不到它的存在。

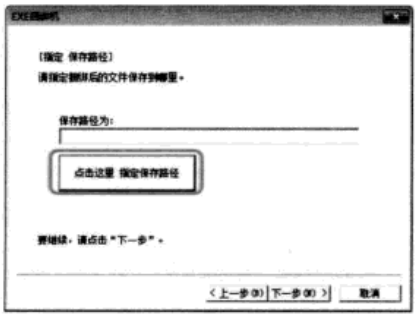


步骤5 弹出【请指定第二个可执行文件】对话框，载入一个木马文件，捆绑后不会看到它的存在，然后单击 打开(O) 按钮。


步骤6 返回【指定 第二个可执行文件】对话框，此时已经添加木马程序了，然后单击 下一步(N) > 按钮。

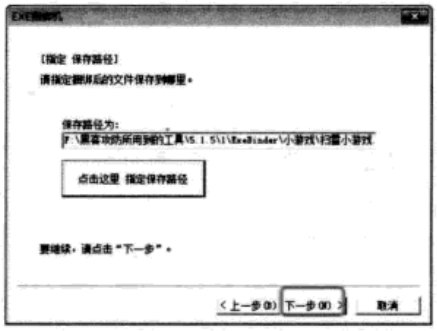



步骤7 弹出【指定 保存路径】对话框，然后单击 点击这里 指定保存路径 按钮。

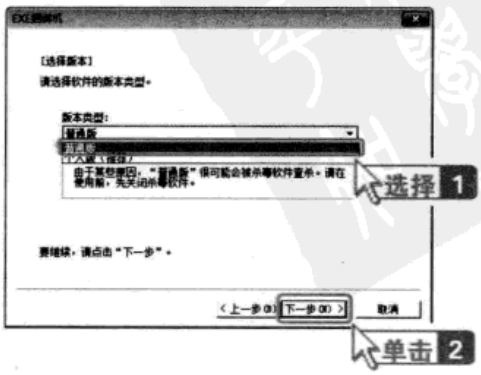



步骤8 弹出【保存为】对话框，选择好保存位置，并在【文件名】文本框中输入一个文件名，这里输入“扫雷小游戏.exe”，然后单击 保存(S) 按钮。

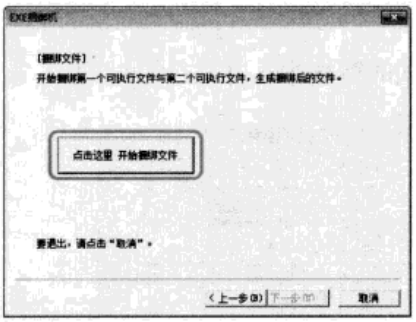

步骤9 返回【指定 保存路径】对话框，此时设置的文件保存路径已经显示在其中了，然后单击 下一步(N) > 按钮。




步骤10 弹出【选择版本】对话框，在【版本类型】下拉列表中选择一种版本类型，这里选择【普通版】选项，然后单击 下一步(N) > 按钮。需要注意的是：“普通版”很可能会被杀毒软件查杀，所以需要先关闭杀毒软件。

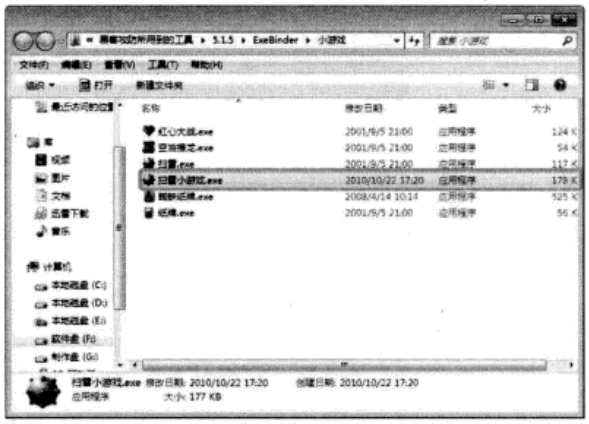


步骤11 弹出【 捆绑文件 】对话框，单击 点击这里 开始捆绑文件 按钮。




步骤12 弹出提示对话框，提示用户捆绑成功，单击 确定 按钮即可。


步骤13 弹出生成的文件所在的文件夹窗口，此时可以看到生成的带有木马的文件与第一个载入的.exe文件图标十分相似，当其他用户运行此程序时，木马程序就在后台悄悄地运行了。

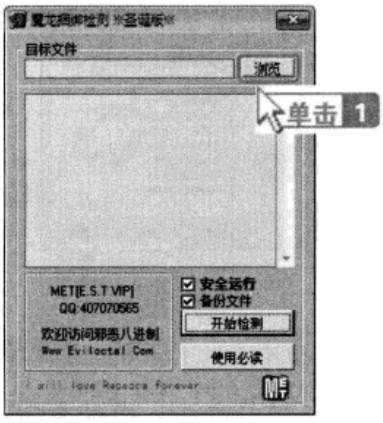


## 捆绑木马的查杀

常见的检测木马捆绑的软件有魔龙捆绑检测工具、荣成文件捆绑克星和FBFD等，下面介绍如何使用魔龙捆绑检测工具软件检测和查杀捆绑木马。具体的操作步骤如下。

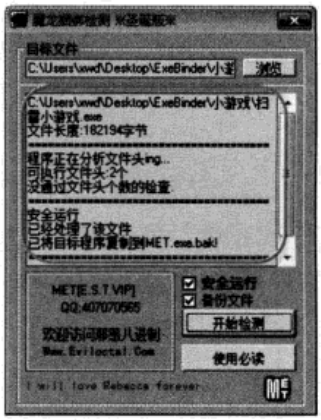
步骤1 下载魔龙捆绑检测工具软件，并双击运行该软件，打开该软件的界面，然后单击 浏览 按钮。

步骤2 弹出【 打开 】对话框，找到想要检测的EXE文件并选中，这里选中前面捆绑的“扫雷小游戏.exe”文件，接着单击 打开(O) 按钮。




步骤3 返回魔龙捆绑检测工具软件的工作界面，可以看到已经选择了该文件。需要注意的是，这里默认选中了【安全运行】和【备份文件】复选框，其目的就是确保文件安全运行并将其备份。然后单击 开始检测 按钮。

步骤4 进入自动检测阶段，稍后检测的结果会显示在中间的窗格中，并进行了处理。


## 2. 自解压木马

自解压木马可以利用WinRAR软件的自解压技术制作。

### 自解压木马的制作

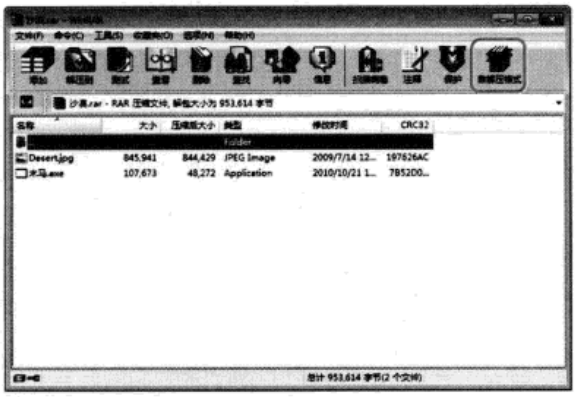
利用WinRAR软件制作自解压木马的具体步骤如下。

步骤1 WinRAR软件用途很广，没有安装此软件的用户可以自行安装。这里用一张图片和一个木马制作自解压木马为例进行介绍，先将这两个文件同时选中，单击鼠标右键，在弹出的快捷菜单中选择【添加到压缩文件】菜单项。


步骤2 弹出【压缩文件名和参数】对话框，在【压缩文件名】文本框中设置文件名，并单击 确定 按钮。

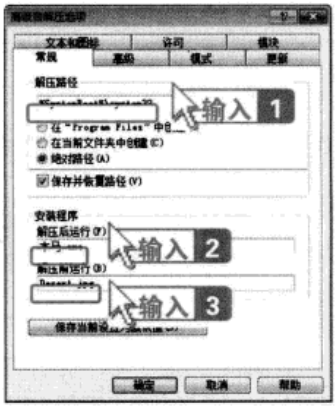

步骤3 在当前的文件夹中生成一个压缩文件，然后双击此压缩文件。

步骤4 弹出一个解压文件的窗口，此时可以看到木马文件和图片文件都显示在其中，单击工具栏中的按钮。

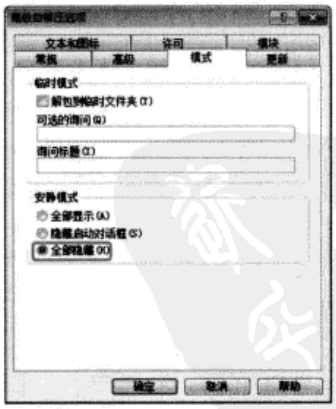


步骤5 在弹出的对话框中切换到【自解压格式】选项卡，单击 高级自解压选项(V)... 按钮。

步骤6 弹出【高级自解压选项】对话框，此时需要在【解压路径】文本框中输入一个路径，该路径可以随意填写，但最好是不容易被发现的位置。例如，输入“%SystemRoot%\system32”，表示解压到系统文件夹下的system32文件夹中，在下侧的【安装程序】组合框中的【解压后运行】文本框中输入木马文件“木马.exe”，在【解压前运行】文本框中输入图片文件“Desert.jpg”。




步骤7 切换到【模式】选项卡，在【安静模式】组合框中选中【全部隐藏】单选钮。



步骤8 切换到【更新】选项卡，在【覆盖方式】组合框中选中【覆盖所有文件】单选钮，单击 确定 按钮。

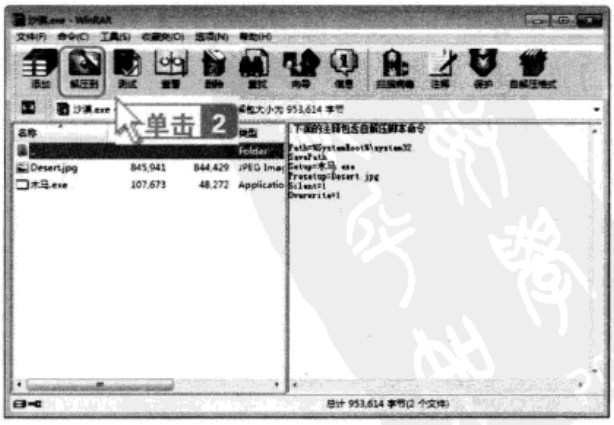

步骤9 返回【压缩文件 沙漠.rar】对话框，单击 确定 按钮即可完成设置，在当前的文件夹中出现了【沙漠.exe】文件，这个就是生成的自解压木马。

### 自解压木马的查杀

用户可以使用最新的杀毒软件对自解压木马进行查杀，具体的操作步骤如下。

步骤1 选中自解压文件，单击鼠标右键，在弹出的快捷菜单中选择【用WinRAR打开】菜单项。

步骤2 弹出【沙漠.exe】对话框，可以看到自解压文件的组成，不难发现其中有.exe文件，单击 按钮，木马程序就不会自动运行了，然后用户就可以提取想要使用的部分，将其他的没有用到的文件全部删除即可。


## 5.2 病毒攻防

计算机病毒泛滥的今天，用户的计算机无时无刻不处在病毒的威胁之下，而大多数用户对计

算机病毒并没有清楚的认识。

## 5.2.1 认识计算机病毒

现在，网络和人们的生活息息相关，在这个信息爆炸的网络时代，计算机病毒也泛滥成灾，下面介绍病毒的相关知识。

### 1. 什么是计算机病毒

使用计算机的用户可能都遭遇过病毒，现在人们往往谈“毒”色变，那么究竟什么是计算机病毒呢？

计算机病毒（Computer Virus）在《中华人民共和国计算机信息系统安全保护条例》中被明确定义，病毒指“编制或者在计算机程序中插入的破坏计算机功能或者破坏数据，影响计算机使用并且能够自我复制的一组计算机指令或者程序代码”。而在一般教科书及通用资料中被定义为：利用计算机软件与硬件的缺陷，由被感染机内部发出的破坏计算机数据并影响计算机正常工作的一组指令集或程序代码。也就是说，计算机病毒是一个程序，一段可执行代码。它会对计算机的正常使用进行破坏，使计算机无法进行正常运行，甚至使整个操作系统或者计算机硬盘损坏。

### 2. 计算机病毒的特征

计算机病毒的作用决定计算机病毒的结构和特征，一般计算机病毒都有如下特征。

#### ● 寄生性

计算机病毒寄生在其他程序之中，当执行这个程序时，病毒就起破坏作用，而在未启动这个程序之前，病毒是不易被人发觉的。

#### ● 传染性

计算机病毒不但具有破坏性，更有害的是具有传染性，一旦病毒被复制或产生变种，其传播速度之快令人难以预防。传染性是病毒的基本特征。

计算机病毒通过各种渠道从已被感染的计算机扩散到未被感染的计算机，在某些情况下造成被感染的计算机工作失常甚至瘫痪。与生物病毒不同的是，计算机病毒是一段人为编制的计算机程序代码，这段程序代码一旦进入计算机并得以执行，它就会搜寻其他符合其传染条件的程序或存储介质，确定目标后再将自身代码插入其中，达到自我复制的目的。如果一台计算机染毒，不及时处理，那么病毒会在这台计算机上迅速扩散，其中的大量文件（一般是可执行文件）会被感染。而被感染的文件又成了新的传染源，再与其他计算机进行数据交换或通过网络接触，病毒会继续进行传染。正常的计算机程序一般是不会将自身的代码强行连接到其他程序上的，而病毒却能使自身的代码强行传染到一切符合其传染条件的未受到传染的程序上。

计算机病毒可通过各种可能的渠道，如U盘、计算机网络去传染其他的计算机。当用户在一台计算机上发现了病毒时，往往曾在这台计算机上用过的U盘也已感染上了病毒，而与这台计算机联网的其他计算机也许也被该病毒染上了。是否具有传染性是判断一个程序是否为计算机病毒的最重要条件。病毒程序通过修改磁盘扇区信息或文件内容并把自身嵌入到其中的方法达到病毒的传染和扩散。被嵌入的程序叫做宿主程序。

### 潜伏性

有些病毒像定时炸弹一样，什么时间发作是预先设计好的。例如，“黑色星期五”病毒，不到预定时间一点都觉察不出来，等到条件具备的时候就爆炸开来，对系统进行破坏。一个编制精巧的计算机病毒程序，进入系统之后一般不会马上发作，可以在几周或者几个月内甚至几年内隐藏在合法文件中，对其他系统进行传染，而不被人发现。潜伏性越好，其在系统中存在的时间就会越长，病毒的传染范围就会越大。潜伏性的第一种表现是指，不用专用检测程序无法检查出病毒程序，因此病毒可以静静地在磁盘或磁带里待上几天，甚至几年，一旦时机成熟，得到运行机会，就又要四处“繁殖”、扩散，继续危害。潜伏性的第二种表现是指，计算机病毒的内部往往有一种触发机制，不满足触发条件时，计算机病毒除了传染外不做其他破坏操作。触发条件一旦得到满足，有的在屏幕上显示信息、图形或特殊标识，有的则执行破坏系统的操作，如格式化磁盘、删除磁盘文件、对数据文件进行加密、封锁键盘以及使系统死锁等。

### 隐蔽性

计算机病毒具有很强的隐蔽性，有的可以通过病毒软件检查出来，有的根本检查不出来，有的时隐时现、变化无常，这类病毒处理起来通常很困难。

### 破坏性

计算机中毒后，可能会导致正常的程序无法运行，计算机内的文件可能会被删除或受到不同程度的损坏。通常表现为：增加、删除、修改、移动。

### 计算机病毒的可触发性

病毒因某个事件或数值的出现，诱使病毒实施感染或进行攻击的特性称为可触发性。为了隐蔽自己，病毒必须“潜伏”，少做“动作”。如果完全不动，一直潜伏的话，病毒既不能感染也不能进行破坏，便失去了杀伤力。病毒既要隐蔽又要维持杀伤力，就必须具有可触发性。病毒的触发机制就是用来控制感染和破坏动作的频率的。病毒具有预定的触发条件，这些条件可能是时间、日期、文件类型或某些特定数据等。病毒运行时，触发机制检查预定条件是否满足，如果满足，启动感染或破坏动作，使病毒进行感染或攻击；如果不满足，则使病毒继续潜伏。

## 5.2.2 病毒的分类

前面已经认识了计算机病毒，那么计算机病毒又有哪些种类呢？它们各自又有什么危害呢？下面介绍计算机病毒的分类。

### 1. 引导型病毒

引导型病毒是一种在ROM BIOS之后，系统引导时出现的病毒，它先于操作系统启动，依托的环境是BIOS中断服务程序。引导型病毒利用操作系统的引导模块放在某个固定的位置，并且控制权的转交方式是以物理位置为依据而不是以操作系统引导的内容为依据。因而病毒占据该物理位置可获得控制权，而将真正的引导区内容转移或替换，待病毒程序执行后，将控制权交给真正的引导区内容，使得这个带病毒的系统看似正常运转，而病毒已隐藏在系统中并伺机传染、发作。

引导型病毒按其寄生位置不同又可分为两类，即MBR（主引导区）病毒和BR（引导）病毒。MBR病毒也称为分区病毒，该病毒寄生在硬盘分区中主引导程序所占据的硬盘0头0柱面第1个扇区中。典型的MBR病毒有大麻（Stoned）、2708、INT60病毒等。BR病毒寄生在硬盘逻辑0扇区（即0柱面0磁道第1个扇区）中，典型的BR病毒有Brain、小球病毒等。

引导型病毒的主要特点如下。

(1) 引导型病毒是在安装操作系统之前进入内存的，寄生对象相对固定，因此该类型病毒基本上不得不采用减少操作系统所占据的内存容量方法来驻留内存高端。而正常的系统引导程序一般是不减少系统内存的。

(2) 引导型病毒需要把病毒传染给软盘，一般通过修改INT 13H的中断向量，而新INT 13H中断向量段址必定指向内存高端的病毒程序。

(3) 引导型病毒感染硬盘时，必定驻留硬盘的主引导扇区或引导扇区，并且只驻留一次，因此引导型病毒一般都是在软盘启动过程中把病毒传染给硬盘的。而正常的引导过程一般不对硬盘主引导区或引导区进行写盘操作。

(4) 引导型病毒的寄生对象相对固定，把当前的系统主引导扇区和引导扇区与干净的主引导扇区和引导扇区进行比较，如果内容不一致，可认定系统引导区异常。

### 2. 木马病毒

木马程序是目前比较流行的病毒文件，与一般的病毒不同，它不会自我繁殖，也并不“刻意”地去感染其他文件，它通过将自身伪装起来以吸引用户下载执行，为施种木马者打开被种者计算机的门户，使施种者可以任意毁坏、窃取被种者的文件，甚至远程操控被种者的计算机。

木马与计算机网络中常常要用到的远程控制软件有些相似，但由于远程控制软件是“善

意”地控制，因此通常不具有隐蔽性；木马则完全相反，木马要达到的是“偷窃”性的远程控制，如果没有很强的隐蔽性的话，那就是“毫无价值”的。它是指通过一段特定的程序( 木马程序 )来控制另一台计算机。木马通常有两个可执行程序：一个是客户端，即控制端，另一个是服务端，即被控制端。植入被种者计算机的是“服务器”部分，而所谓的黑客正是利用控制器进入运行了服务器的计算机。运行了木马程序的服务器以后，被种者的计算机就会有一个或几个端口被打开，使黑客可以利用这些打开的端口进入计算机系统，安全和个人隐私也就全无保障了。木马的设计者为了防止木马被发现，采用了多种手段隐藏木马。

木马的服务器一旦运行并被控制端连接，其控制端将享有服务端的大部分操作权限，例如，给计算机增加口令，浏览、移动、复制、删除文件，修改注册表，更改计算机配置等。

随着病毒编写技术的发展，木马程序对用户的威胁越来越大，尤其是一些木马程序采用了极其狡猾的手段来隐蔽自己，使普通用户很难在中毒后发觉。

木马病毒有以下危害。

(1) 盗取网游账号，威胁虚拟财产的安全。

(2) 盗取网银信息，威胁真实财产的安全。

(3) 利用即时通信软件盗取身份，传播木马病毒。

(4) 给计算机打开后门，使计算机可能被黑客控制。

### 3. 可执行文件病毒

可执行文件病毒依附在可执行文件或覆盖文件中，当病毒程序感染一个可执行文件时，病毒会修改原文件的一些参数，并将病毒自身程序添加到原文件中。

当执行被感染病毒的文件时，由于病毒修改了一些参数，所以首先执行的是病毒程序的代码，此段程序代码主要实现将病毒程序驻留在内存，以取得操作系统的控制权，从而可以完成病毒的复制和一些破坏操作。最后再执行原文件的程序代码，实现原程序的功能来迷惑用户。

可执行文件病毒主要感染系统的可执行文件，如Windows系统的.com或.exe文件或者覆盖文件，又或者.dll文件，但极少感染数据文件。

当感染了病毒的可执行文件被执行或当系统有任何读写操作时，病毒就会向外扩散。

### 4. 多形性病毒

多形性病毒又称幽灵病毒，这类病毒使用一个复杂的算法，使自己每传播一份都具有不同的内容和长度。它们一般由一段混有无关指令的解码算法和被变化过的病毒体组成。

此种病毒主要是针对杀毒软件而设计的，所以新型的多形性病毒往往可以躲避杀毒软件的查杀，甚至出现杀毒软件误报的情况。

### 5. 语言病毒

语言病毒是利用Java、Visual Basic、HTML、JavaScript和ActiveX的特性来编写的病毒，此种病毒虽不能破坏硬盘上的数据，但如果用户使用浏览器来浏览带有这些病毒的网页时，在不知不觉中，病毒已经进入了计算机进行复制，并通过网络窃取用户秘密信息，如网银账号等。

### 6. 混合型病毒

混合型病毒是指具有引导型病毒和文件型病毒寄生方式的计算机病毒，所以它的破坏性更大，传染的机会也更多，杀灭也更困难。这种病毒扩大了病毒程序的传染途径，它既感染磁盘的引导记录，又感染可执行文件。当染有此种病毒的磁盘用于引导系统或调用执行染毒文件时，病毒都会被激活。因此在检测、清除混合型病毒时，必须全面彻底地根治，如果只发现该病毒的一个特性，把它只当做引导型或文件型病毒进行清除。虽然好像是清除了，但还留有隐患，这种经过消毒后的“洁净”系统更赋有攻击性。混合型病毒有Flip病毒、新世际病毒、One-half病毒等。

## 5.2.3 病毒诊断

在网络时代，病毒是层出不穷、无所不在的，在变化多端的计算机病毒侵袭下，中毒是不可避免的。

### 1. 计算机中毒的表现

怎么判断计算机是否中毒了呢？其实，计算机中毒和人生病一样，也是有很多表现的，如果计算机出现了这些表现，就基本上可以断定计算机中毒了。

- 系统无法启动

这是因为病毒修改了硬盘的引导信息或者删除了系统文件，甚至破坏了BIOS，例如，CIH病毒。

- 计算机经常死机

这是因为病毒运行了很多程序，或是大量进行自我复制，或是通过邮件和QQ等交流工具大量发送传播，耗尽系统资源，从而造成死机。

- 系统经常提示内存不足

在运行很少程序的情况下，系统经常提示内存不足，这很可能是病毒占用了大量的内存资源。

### 硬盘空间不足

用户在硬盘存放的文件不多，系统却提示硬盘空间不足，出现这种情况的原因很可能是病毒大量自我复制，占用大量的硬盘空间，造成硬盘空间不足。

### 文件无法打开

可执行文件不能运行或者计算机上的文件突然无法打开，这种情况极有可能是因为病毒破坏了可执行文件或者破坏了文件关联，从而造成的文件无法打开。

### 计算机运行速度很慢

计算机的运行速度，以及开机、关机速度都很慢，很有可能是病毒运行占用了大量的系统资源，从而使计算机的运行速度变慢。

### 系统自动加载某些程序

在进行BIOS设置时键盘、鼠标可以正常使用，但在进入系统后无法使用，这很可能是某些病毒锁定了键盘和鼠标，使用户不能正常使用计算机。

### 数据突然丢失

硬盘中突然有大量数据丢失，这很可能是病毒具有删除文件的破坏性，对硬盘中的文件进行删除，从而使大量文件消失，也有可能是病毒加密隐藏文件，把硬盘中的文件加密隐藏了，以便病毒制作者敲诈勒索。

### 系统中突然增加了大量来历不明的文件

在系统中发现了很多来历不明的文件，这可能是病毒的变种，或者是病毒入侵系统时留下的垃圾文件。

### 系统经常出现错误提示

系统经常弹出“内存不能为只读”或“系统出现严重错误”等错误提示，这很可能是病毒破坏了系统文件，造成系统错误。

### 浏览网页时弹出莫名奇妙的网页

在浏览网页时经常弹出一些莫名其妙的网页，并且在浏览一些比较正规的网站，如新浪、百度、谷歌等网站时也弹出这些莫名其妙的网页，这很可能是由于病毒劫持了浏览器而造成的。

### 浏览器的主页莫名其妙地被更改

在用户不知情的情况下，浏览器的主页被更改为莫名其妙的网页，这很可能是病毒为了方便到该网站下载更多的病毒，将用户浏览器的主页更改了。

### 杀毒软件被结束，并且不能启动

杀毒软件被结束，并且不能启动，这也是病毒为了逃避杀毒软件的查杀而造成的。

基本来说，计算机中了病毒会有以上这些表现，但并不是说计算机没有这些表现就一定没有中病毒，有些病毒为了不让用户发现，不会明显地显现出中毒的特征，这就需要用户使用杀毒软件来检查计算机是否中毒。

## 2. 计算机中毒的途径

计算机病毒不是无中生有的，计算机也不可能无缘无故地中毒，它总有一些中毒的途径，下面介绍计算机中毒的途径。

### 下载了带毒的文件

网络上有很多共享信息，用户可能经常到网络上下载一些文件，谁都不能保证这些文件不会带有病毒，在这种情况下，如果下载了带有病毒的文件，而用户又在不知情的情况下打开了该文件，那么用户的计算机就会中毒。其实，这种情况是可以避免的，要预防计算机通过这种途径中毒，用户就需要到正规的网站下载文件，不要到一些不正规的网站下载文件。另外，下载下来的文件一定要经过杀毒软件的查杀后再使用，以免文件带有病毒。

### 浏览了带有病毒的网站

用户每天都要浏览大量的网站以获取自己需要的信息，而用户浏览的这些网站很可能会带有病毒，用户在浏览带有病毒的网站时，自己的计算机也很可能中毒。可以采取以下措施避免在浏览网站时中毒：不要浏览一些不健康的网站，这些网站带有病毒的概率要比正规网站大得多；不要相信一些莫名其妙的中奖信息，没有天上掉馅饼的好事，这些信息链接到的网站很有可能带有病毒，即便没有病毒，也是为了骗取用户的钱财；要开启杀毒软件的实时监控或者主动防御功能，这样可以有效地防止病毒入侵。

### 使用盗版光盘

使用盗版光盘不但是偷窃他人劳动成果的不法行为，而且很有可能会通过盗版光盘中毒，因为盗版光盘的制造者不会保证盗版软件没有病毒，也不会保证在盗版光盘的制造过程中不中毒，甚至有些盗版光盘制造者会在盗版软件中故意带有病毒。用户应尽量使用正版的软件或者

免费软件，不要使用盗版软件，减少通过盗版软件中毒的可能性。

### ● 使用了带有病毒的 U 盘

由于U盘的便捷性及大容量，被越来越多的用户使用，而U盘也成为病毒传播的一个重要途径，特别是AutoRun病毒，更是U盘病毒的“主力军”。这种病毒利用了操作系统的自运行机制，当U盘插入计算机中后，计算机会自运行U盘中的文件，当U盘中带有AutoRun病毒时，病毒就会传播到用户的计算机上，这样用户的计算机也就中毒了。预防这种病毒，用户应该停止操作系统的自运行，使操作系统不再自运行U盘中的内容，并且U盘插入后，不要急于打开，而是应该先用杀毒软件杀毒后再打开U盘。

### ● 阅览了带有病毒的电子邮件

电子邮件是网上交流的一种重要方式，也是人们现在常用的商务手段，同样，电子邮件也是病毒传播的重要途径，一旦某个用户感染了邮件病毒，这种病毒就会自动从地址簿中寻找邮件地址，并给找到的地址发送病毒邮件，收到邮件的人打开这些病毒邮件后，也就中毒了。预防这种病毒的方法是尽量不要查看陌生人发送的电子邮件。现在的杀毒软件大部分都带有邮件监控功能，用户应该开启该功能，以预防带毒邮件。

### ● 通过聊天工具接收了带有病毒的文件

现在人们在网上交流离不开聊天工具软件，而聊天工具软件也成为病毒传播的一条重要途径，病毒可以给好友发送带有病毒的文件，一旦用户打开了这些文件，计算机就中毒了。对付这种病毒的主要手段是不要接收陌生人发送的文件，即便是好友发送的，也要先用杀毒软件查杀，确定没有带毒后再打开。

### ● 受到了黑客的入侵

黑客入侵也是病毒传播的重要途径。他们可以入侵用户的计算机，使病毒在用户的计算机上运行，预防黑客入侵的主要手段就是设置好防火墙，但实际上，黑客入侵是防不胜防的，这就需要用户经常使用杀毒软件查杀病毒，防止自己的计算机上有病毒运行。

## 5.2.4 病毒防范

网络病毒的快速发展让人防不胜防，一不小心就会陷入病毒的陷阱。采取相应的防范措施并及时查杀病毒是每一位用户必须要具备的基本能力。

### 1. 主要的防范方法

病毒的防范很重要，下面介绍一些主要的防范方法。

### 不打开来历不明的邮件附件

不要打开来历不明的邮件附件，即使扩展名看起来没有危险，也不要打开，因为Windows允许在文件名后使用多个后缀，也就是说，用户看到的如“.doc”的文件很有可能是“.doc.exe”文件。

### 安装并及时更新杀毒软件

安装并及时更新杀毒软件。这是因为病毒的更新速度很快，只有最新的杀毒软件才能保护计算机的安全。

### 只从可信站点下载软件

对于网络用户来说，从网上下载一些软件是常有的事，但很难判断这些软件是否是可信的，一般从一些知名的软件站点，如华军软件园等站点进行下载，并在下载完成后先进行病毒扫描。

### 不共享文件

文件共享是导致病毒从一台计算机传播到另一台计算机的有效途径，为了防御病毒，在共享文件时要进行杀毒扫描。

### 扫描移动存储设备

当使用软盘、光盘、闪存盘和移动硬盘等移动存储设备时，要用杀毒软件扫描后才可以打开使用，以防病毒通过移动存储设备传播。

### 安装使用防火墙

网络已成为人们日常生活中的一部分，所以安装使用个人防火墙是非常重要的。这样可以保护个人隐私并阻止黑客的入侵。

## 2. 常见的杀毒软件

计算机病毒可以说是防不胜防，谁都不能保证自己的计算机不会中毒，所以病毒的查杀和预防十分重要，而这离不开杀毒软件。

目前国内常用的杀毒软件有以下几种。

### 瑞星杀毒软件

瑞星杀毒软件是由国内最大的信息安全厂商——瑞星公司出品的，它的特点是符合中国人

的使用习惯，病毒库是国产杀毒软件中最大的，但提示窗口较多，查杀能力较卡巴斯基等稍弱。

- 江民杀毒软件

江民杀毒软件是江民新科技术有限公司推出的杀毒软件，它的杀毒能力较强，性能不错，但病毒库相比其他杀毒软件不是太齐全。

- 金山毒霸

金山毒霸是由金山公司推出的杀毒软件，它的设置简单，适合新手使用，但查杀能力稍弱。

- 卡巴斯基

卡巴斯基是由俄罗斯卡巴斯基实验室推出的信息安全产品。它的主要特点是杀毒引擎技术先进，查杀病毒能力强，病毒库更新速度快，有世界上最全的病毒库，但占用系统资源较多，查杀速度较慢。

- 诺顿

诺顿是赛门铁克（Symantec）公司推出的信息安全产品之一，也是一个应用广泛的反病毒程序。该产品发展至今，除了原有的防毒功能外，还有防间谍等网络安全风险的功能。它的主要特点是从系统底层查杀病毒，查杀能力强大，减少窗口弹出，给用户提供静默的防护体验，但占用资源较多，查杀速度较慢，适合企业用户使用。

- Macfee

它是由世界第八大独立软件公司——美国Macfee公司推出的反病毒产品，它的特点是占用资源相对较少，防御能力较强；但对病毒的查杀能力较卡巴斯基等稍弱。

## 5.3 恶意代码攻防

随着网络的使用越来越广泛，针对浏览器漏洞或者浏览器特殊功能的恶意代码也越来越多，这些恶意代码可能会对用户的计算机进行有害的操作，认识并防范这些恶意代码也成为网络时代的必修课。

### 5.3.1 认识恶意代码

现今，由于恶意代码的存在，在Internet上不经意地打开一个网站就有可能使用户的计算机感染上病毒，造成首页被篡改、浏览器被破坏甚至硬盘被格式化等不可预料的严重后果，因此

用户掌握这方面的知识是很有必要的。

### 1. 恶意代码的定义和特征

恶意代码在网络上非常常见，那么究竟什么是恶意代码呢？它又有哪些特征呢？下面简单介绍一下。

#### 恶意代码的定义

恶意代码（malicious code）是一段程序，它会在用户不察觉的情况下嵌入另一个程序中，从而达到破坏计算机的数据、运行具有入侵性或破坏性的程序及破坏被感染计算机数据的安全性和完整性的目的。

#### 恶意代码的特征

恶意代码的编写大多是出于商业或探测他人资料的目的，如宣传某个产品、提供网络收费服务或对他人的计算机直接进行有意的破坏等，总的来说，它具有恶意破坏的目的、其本身为程序，以及通过执行发生作用3个特征。

(1) 恶意破坏的目的。

有相当一部分黑客进行恶意代码攻击的目的是从破坏其他用户的系统中得到“成就感”。但现在更多的黑客则是出于经济利益。例如，某些广告类代码可以通过用户的上网习惯以提高广告点击率来获取经济利益，而更直接的则是通过窃取其他用户的网上信用卡、银行代码等直接对其进行经济侵犯。现今又出现了潜伏性的恶意代码，在攻击的同时尽量不被发现，对用户和社会都造成了严重的危害，构成了严重的经济犯罪。

(2) 其本身为程序。

恶意代码是一段程序，它可以在很隐蔽的情况下嵌入另一个程序中，通过运行别的程序而自动运行，从而达到破坏被感染计算机的数据、程序以及对被感染计算机进行信息窃取等目的。

(3) 通过执行发生作用。

恶意代码与木马一样，只要用户运行就会发作，只不过恶意代码是通过网页进行传播的。

### 2. 恶意代码的传播方式和趋势

恶意代码按传播方式可以分为病毒、蠕虫、木马、移动代码和间谍软件等。其传播的目的已有所变化，传统的攻击活动常常是受好奇心驱使，希望自己的技术可以得到认可，而现在的攻击则以获得经济利益为目的。这些攻击通常为犯罪行为，例如，为牟取经济利益而非法盗取他人的信息，从而对其造成经济损失。

## 恶意代码的传播方式

总的来说，恶意代码的传播是因为用户的软件出现了漏洞、操作不慎或者是两者的结合造成。

(1) 病毒。

病毒具有自我复制的功能，一般嵌入主机的程序中。当被感染文件执行操作，例如，用户打开一个可执行文件时，病毒就会自我繁殖。病毒一般都具有破坏性。

(2) 木马。

这种程序从表面上看没有危害，但实际上却隐含着恶意的意图和破坏的作用。一些木马程序会通过覆盖系统中已经存在的文件的方式存在于系统之中；另外有的还会以软件的形式出现，因为它一般是以一个正常的应用程序身份在系统中运行的，所以这种程序通常不容易被发现。

(3) 蠕虫。

蠕虫是一种可以自我复制的完全独立的程序，它的传播不需要借助被感染主机中的其他程序和用户的操作，而是通过系统存在的漏洞和设置的不安全性来进行入侵，如通过共享的设置来侵入。蠕虫可以自动创建与它的功能完全相同的副本，并能在无人干涉的情况下自动运行，大量地复制占用计算机的空间，使计算机的运行缓慢甚至瘫痪。其中比较典型的有Blaster和SQL Slammer。

(4) 移动代码。

移动代码是能够从主机传输到客户端计算机上并执行的代码，它通常是作为病毒、蠕虫或者是特洛伊木马的一部分被传送到客户的计算机上的。此外，移动代码还可以利用系统的漏洞进行入侵，如非法的数据访问和盗取管理员账号等。

(5) 间谍软件。

散布间谍软件的网站或个人会使用各种方法使用户下载间谍软件并将其安装在他们的计算机上。这些方法包括创建欺骗性的免费服务，以及隐蔽地将间谍软件和用户可能需要的其他软件捆绑在一起等，如使用免费的共享软件，达到利用软获取经济利益等目的。

## 恶意代码的传播趋势

(1) 种类更多。

恶意代码的传播不再单纯地依赖软件漏洞或者他人操作中的不慎，也有可能是两者的结合，如蠕虫产生寄生的文件病毒、特洛伊木马程序、口令窃取程序、后门程序等，这进一步模糊了蠕虫、病毒和特洛伊木马之间的区别。

(2) 利用混合传播模式。

“混合病毒威胁”和“收敛威胁”已成为新的病毒术语，红色代码利用的就是IIS的漏洞，

它们的特点都是利用软件漏洞，以病毒的模式从引导区方式发展为多种类病毒方式进行攻击。

(3) 跨平台攻击。

跨平台攻击已开始出现，有些恶意代码对所有的平台都能够起作用，例如，代码能兼容Windows、UNIX及Linux平台并进行攻击。

(4) 使用销售技术。

另外一个趋势是更多的恶意代码使用销售技术，其目的不仅在于利用受害者的邮箱实现最大数量的信息转发，而且要引起受害者的兴趣，让受害者进一步对恶意代码进行下载等操作，并且使用网络探测和电子邮件脚本嵌入等技术来达到目的。

(5) 服务器和客户机同样受到攻击。

对于现今的恶意代码，服务器和客户机的区别越来越模糊，客户计算机和服务器如果运行同样的应用程序，也将会受到恶意代码的攻击。

(6) Windows操作系统被攻击得最频繁。

Windows操作系统更容易遭受恶意代码的攻击，它也是病毒攻击最集中的平台，病毒总是选择配置不好的网络共享和服务作为进入点。

(7) 恶意代码类型变化。

恶意代码利用MIME边界和UUEncode头的处理薄弱的缺陷，将恶意代码伪装成安全的数据类型，欺骗用户执行代码。

## 5.3.2 恶意代码分析

恶意代码主要是通过嵌入在网页中的代码来修改浏览者的注册表而起破坏作用的，例如修改IE首页和修改IE右键菜单等，下面针对上述的情况介绍检测和解决的办法。

### 1. 修改 IE 首页

修改IE首页是恶意代码最常见的一种攻击方式，也是恶意网站和病毒惯用的手法，目的是增加其网站流量，并偷偷安装木马。

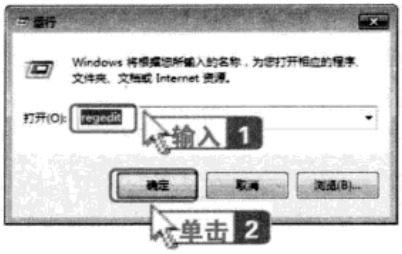
IE首页对应在注册表的分支是HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\Start Page，Start Page中的值就是恶意代码修改IE首页的值。

下面介绍解决恶意代码修改IE首页的具体步骤。

步骤1 选择【开始】➢【运行】菜单项，打开【运行】对话框，在【打开】文本框中输入“regedit”，然后单击 确定 按钮。

步骤2 打开【注册表编辑器】窗口，在左侧的窗格中找到HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main选项，选择【Main】选项，在右侧窗格的【Start Page】选项上单击

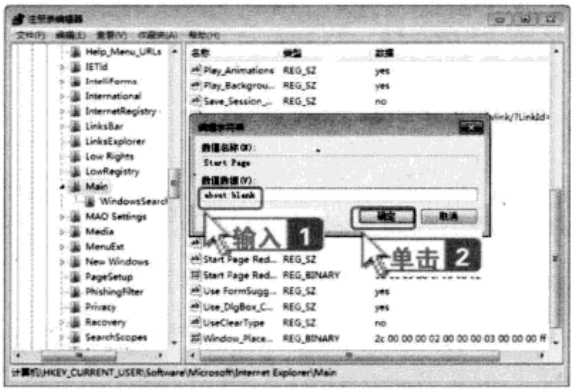
鼠标右键，在弹出的快捷菜单中选择【修改】菜单项。





步骤3 打开【编辑字符串】对话框，在【数值数据】文本框中把篡改的IE首页删除，在【数值数据】文本框中输入“about:blank”，表示首页为空白页，单击 确定 按钮即可。

步骤4 修改完成后，打开IE浏览器进行查看，发现首页已经变成了空白页，恢复了正常。




## 2. 修改 IE 右键菜单

修改IE右键菜单的注册表分支为HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\MenuExt，MenuExt注册表项下面的就是IE右键菜单所包含的组件和恶意广告插件。解决的方法同解决修改IE首页的方法相似。

打开注册表并找到HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\MenuExt分支，选中含有恶意代码的IE右键菜单项，然后单击鼠标右键，在弹出的快捷菜单中选择【删除】菜单项即可。


此时打开IE浏览器进行检测，用户会发现含有恶意代码的菜单项在IE右键菜单中消失了（修改后需要重新打开IE浏览器才有效）。

恶意代码对注册表的修改远远不止是上面的两个例子，所以用户最好禁止注册表的使用，当需要使用时再打开。对于禁止注册表的使用，用户利用组策略进行设置即可。

### 5.3.3 恶意代码防范

下面介绍恶意代码的预防和查杀。

#### 1. 恶意代码的预防

恶意代码的预防主要注意下面几个方面。

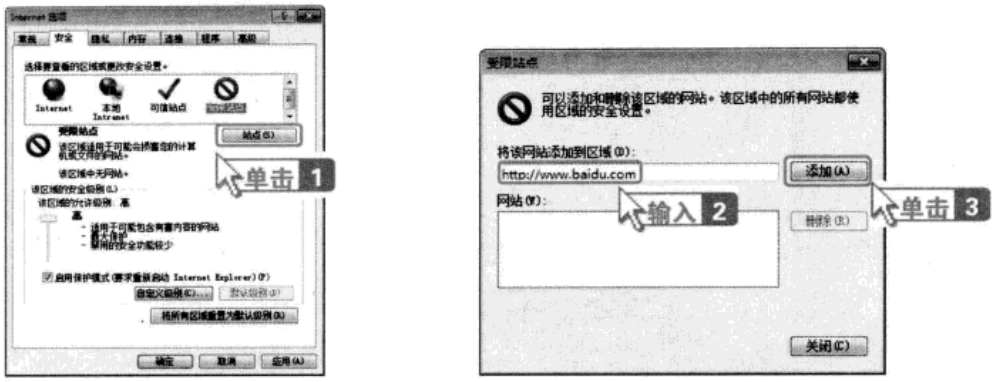
(1) 若要避免被网页恶意代码感染，关键是不要轻易打开一些不太熟悉的网站，尤其是一些不健康的网站，否则不经易间就会误入网页代码的圈套。

(2) 打开IE浏览器，选择【工具】➢【Internet选项】菜单项，打开【Internet选项】对话框，切换到【安全】选项卡，在【该区域的安全级别】组合框中拖动滑块把安全级别调至最高。

(3) 一定要在计算机上安装网络防火墙，并要时刻打开实时监控功能。

(4) 将一些恶意的网站添加到受限的站点中。打开IE浏览器，选择【工具】➢【Internet选项】菜单项，打开【Internet选项】对话框，切换到【安全】选项卡，在【选择要查看的区域或更改安全设置】组合框中选择【受限站点】选项，然后单击 站点(S) 按钮，打开【受限站点】对话框，用户可以在【将该网站添加到区域】文本框中输入恶意网站的地址，然后单击 添加(A) 按钮即可添加一个恶意站点。用户可以用类似的方法继续添加其他恶

意站点，添加完毕单击 确定 按钮即可。




当用户再次访问该站点时就会受一些限制，并且在状态栏中显示受限站点的标记。

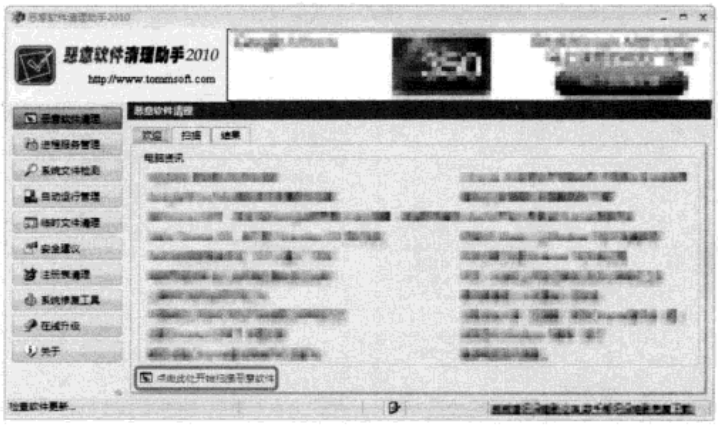

## 2. 恶意软件的查杀

恶意软件的查杀主要依靠软件，具有这样功能的软件很多，如恶意软件清理助手、360安全卫士等，其中，恶意软件清理助手是比较专业的查杀软件。

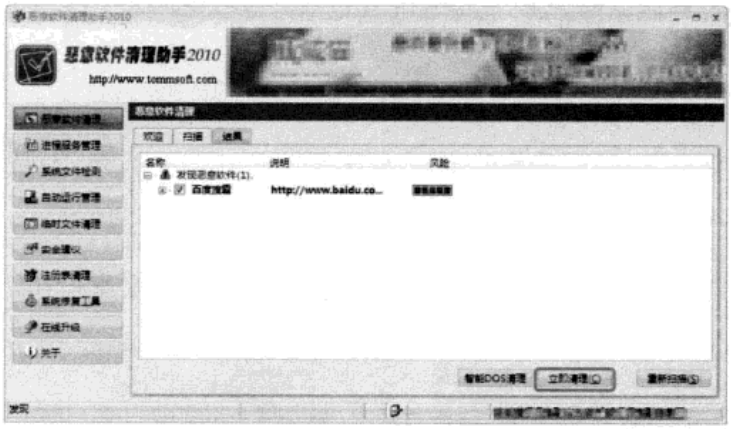
### 利用恶意软件清理助手查杀

恶意软件清理助手为绿色软件，不需要安装，直接将下载的压缩包解压到一个文件夹中即可正常使用。下面介绍使用恶意软件清理助手查杀恶意软件的具体步骤。

步骤1 双击【恶意软件清理助手】图标，运行【恶意软件清理助手2010】程序，单击【点击此处开始扫描恶意软件】链接。




步骤2 稍后进入自动检测的过程中，稍等片刻，检测的结果就会自动显示在窗口中。然后选中所有的恶意插件前面对应的复选框，并单击 立即清理(C) 按钮，随即软件就会删除这些恶意插件。



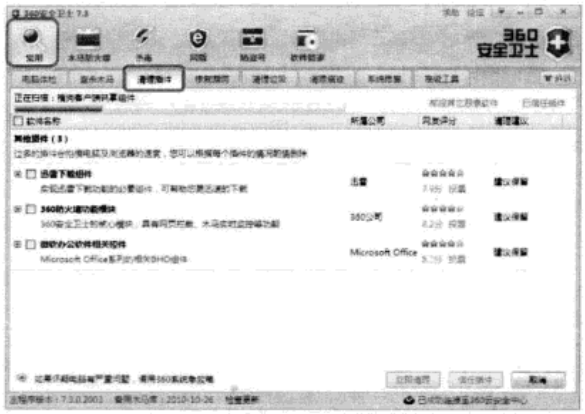

## 利用 360 安全卫士查杀

360安全卫士是一款功能很强大的软件安全类上网辅助软件，它拥有查杀恶意软件、插件管理、病毒查杀、诊断及修复四大主要功能，同时还提供弹出插件免疫，清理使用痕迹以及系统还原等特定辅助功能。利用它可以查杀木马和清理插件功能来查杀恶意软件。

下面介绍使用360安全卫士的清理插件功能来查杀恶意软件的具体步骤。

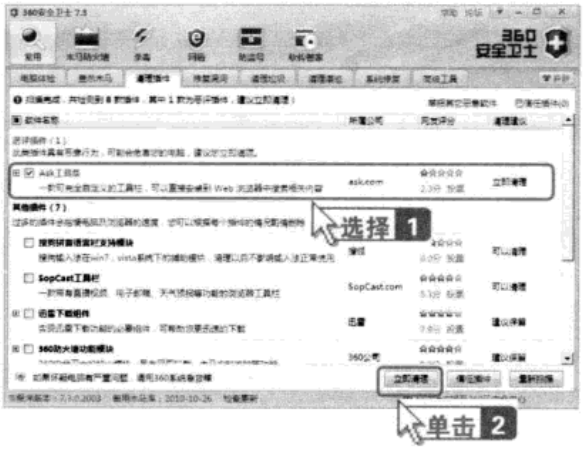
步骤1 运行【360安全卫士】程序，打开【360安全卫士7.3】窗口。

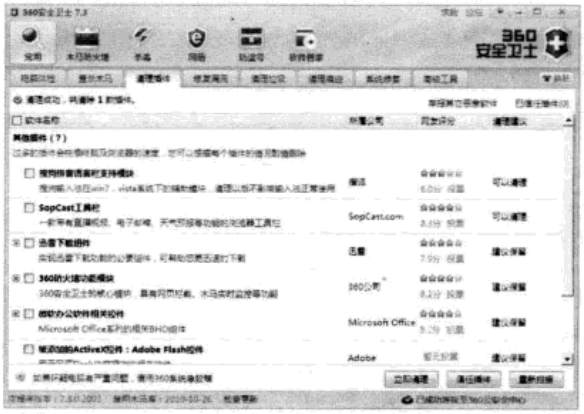
步骤2 单击 按钮，并切换到【清理插件】选项卡，随即进行检测。


步骤3 稍等片刻，检测的结果就会自动显示在窗口中。选中所有的恶意插件前面对应的复选框，并单击 立即清理 按钮。

步骤4 随即软件删除这些恶意插件，稍后便会清理完毕。




## 5.4 U盘病毒攻防

U盘病毒已经是当今病毒中最为流行的一种病毒了，它利用配置文件，使用户的计算机在不经意间就染上了U盘中的病毒，并且传播性非常强，危害性非常大。

### 5.4.1 认识U盘病毒

随着科技的不断发展，电子产品的不断更新，如今U盘已经成为了最主流的移动存储设备，它拥有携带容易、使用方便以及价格便宜等优点，这就使一些黑客把目光转移到了它的身上，现在利用U盘来传播病毒已经是黑客最常用的手段。

### 1. U盘病毒的定义

顾名思义，U盘病毒就是通过U盘传播的病毒，U盘病毒只是习惯用语，它还可以通过U盘、MP3、移动硬盘等移动存储设备传播。自从发现U盘的autorun.inf漏洞之后，U盘病毒的数量与日俱增，到现今可以说是达到泛滥的程度了。

### 2. U盘病毒的攻击原理

该类病毒首先向U盘写入病毒程序，然后更改autorun.inf文件。autorun.inf文件记录用户选择何种程序来打开U盘。如果autorun.inf文件指向了病毒程序，那么Windows就会运行这个程序，引发病毒。一般病毒还会检测插入的U盘，并对其实行上述操作，导致一个新的U盘病毒产生，并且用户的计算机将会被其感染。

### 3. U盘病毒的特征

#### ● 自动运行性

所谓自动运行性，就是利用其配置文件来根据用户的操作习惯使病毒文件自动运行，通常U盘病毒是用户在双击打开U盘时自动运行的。

#### ● 隐藏性

病毒程序不会轻易地让用户发现，一般都是巧妙地存在U盘中的。例如：

(1) 伪装成系统文件隐藏。一般系统文件是看不见的，这样就达到了隐藏的效果。现在的大多数U盘病毒都采取这种隐藏方式。

(2) 藏于系统文件夹中。虽然看似与第一种方式相同，但实际上并不相同。这种系统文件夹一般都具有迷惑性，例如，文件夹的名称为回收站。

(3) 伪装成其他文件的图标。有些病毒程序将自身图标改为其他文件的图标，因为默认情况下计算机中不显示文件的后缀名，或者文件名太长看不到后缀名，所以导致用户误打开。

具有上述3种情况的任意两种方式组合的U盘病毒迷惑性更大，U盘中毒的概率也就更高。

## 5.4.2 防范U盘病毒

U盘病毒的攻防主要包括中毒前的预防和查杀以及中毒后的查杀。

预防U盘病毒的方法很多，下面介绍如何手动预防U盘病毒。

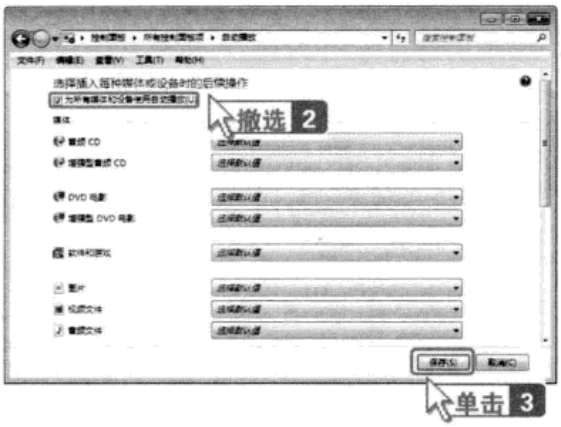
#### ● 关闭自动播放

关闭自动播放是阻止病毒运行的第一步，遏制了病毒的自动运行才能进行下面的工作，所

以关闭自动播放是非常必要且重要的。下面介绍关闭U盘自动播放的具体步骤。

步骤1 单击【开始】菜单按钮，在弹出的快捷菜单中选择【控制面板】菜单项，打开【控制面板】窗口，在该窗口中找到并双击【自动播放】图标。

步骤2 弹出【自动播放】窗口，取消选中【为所有媒体和设备使用自动播放】复选框，然后单击 保存(S) 按钮即可。


## 设置文件夹选项

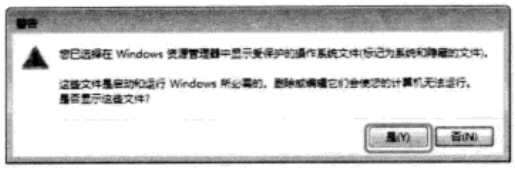
设置文件夹选项的目的是让所有的文件都显示出来，默认情况下用户是看不到隐藏文件和系统保护文件的，而病毒就经常隐藏起来或伪装成系统文件。

下面介绍设置文件夹选项的具体步骤。

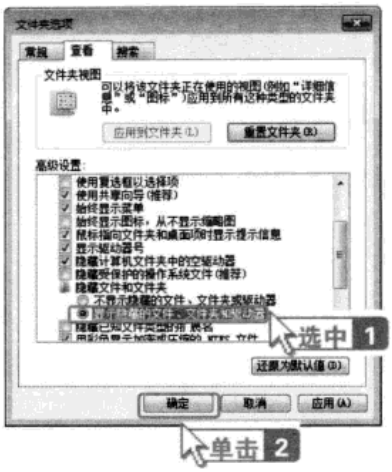
步骤1 单击桌面上的【计算机】图标，打开【计算机】窗口，在菜单栏中选择【工具】➢【文件夹选项】菜单项。

步骤2 打开【文件夹选项】对话框，在【高级设置】列表框中取消选中【隐藏受保护的操作系统文件（推荐）】复选框。

步骤3 弹出【警告】对话框，提示用户在Windows任务管理器中会显示受保护的操作系统文件，并且对这些文件的删除和调整都会使计算机无法运行，单击 是(Y) 按钮即可。




步骤4 返回【文件夹选项】对话框，在【高级设置】列表框中选中【显示隐藏的文件、文件夹和驱动器】单选钮，然后单击 确定 按钮即可。




## 使用软件预防 U 盘病毒

用户还可以使用软件预防 U 盘病毒，下面以常用的 360 安全卫士为例进行介绍。

步骤1 下载并安装最新版本的360安全卫士，然后运行该软件，打开360安全卫士的主窗口，接着单击【木马防火墙】按钮。

步骤2 进入【360木马防火墙】窗口，单击【U盘防火墙】选项后面的 已关闭 按钮，开启U盘病毒免疫功能，此时将U盘插入机箱的USB插槽中，即使其中有病毒也不会自动运行，这样用户就可以放心地对U盘病毒进行查杀了。


## 新手问题解答

### 如何揭露木马的伪装手段

木马经常伪装成为系统文件、图片或者网页等，用户通过查看其后缀名来检查该文件是否为木马程序。

打开【计算机】窗口，选择【工具】➢【文件夹选项】菜单项，打开【文件夹选项】对话框，切换到【查看】选项卡，取消选中【隐藏已知文件类型的扩展名】复选框，然后返回原位置，根据该文件的扩展名来判断是否为木马程序。

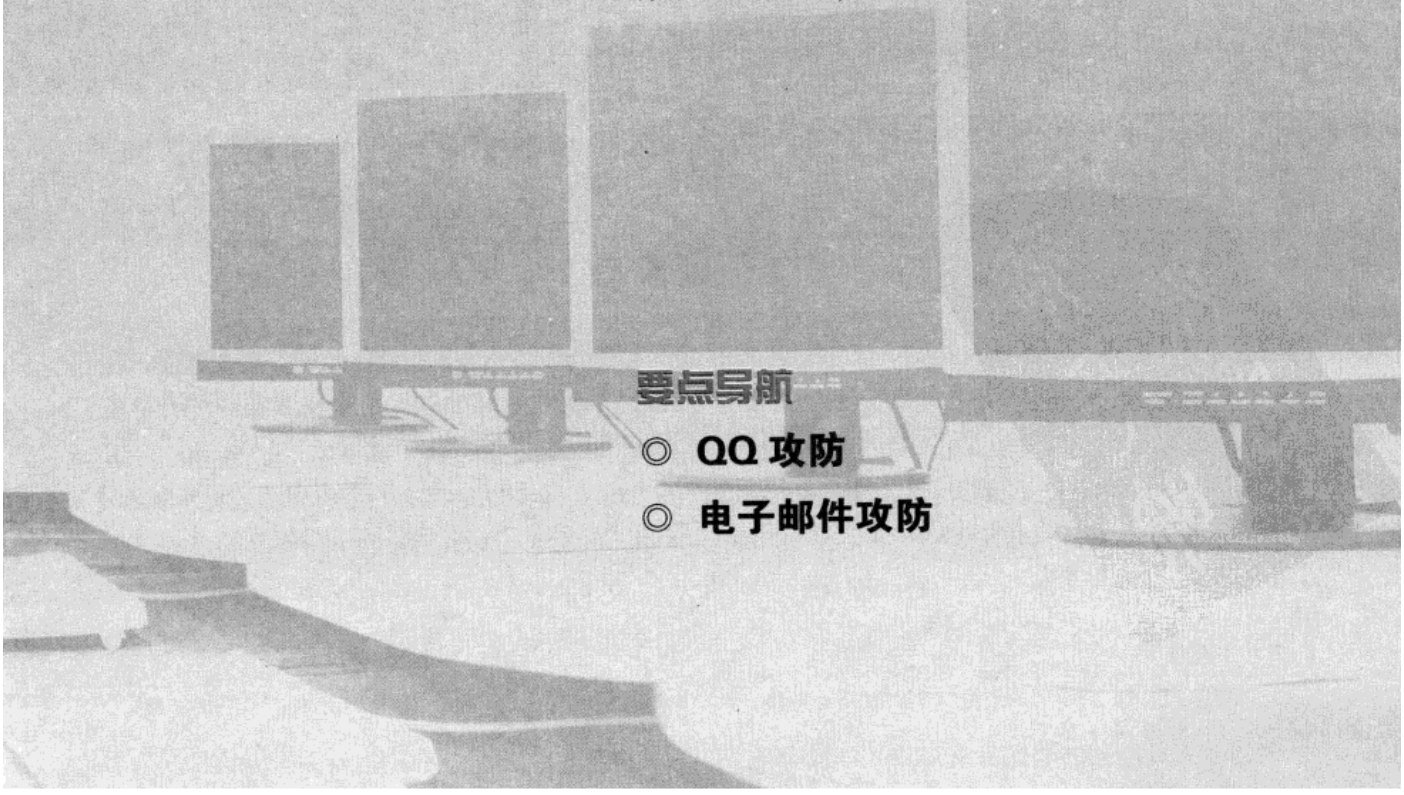
### 如何关闭系统的自动播放功能

关闭系统的自动播放功能能够阻止病毒运行。

打开【控制面板】窗口，在该窗口中打开【自动播放】窗口，然后取消选中【为所有媒体和设备使用自动播放】复选框即可。

# 第6章 网络安全攻防

QQ 在国产聊天软件中占有绝对的主导地位，目前大部分的计算机用户都至少拥有一个 QQ 账户。E-mail 邮箱同样是现在大多数用户最常用的通信方式。QQ 和邮箱账户的安全问题也受到越来越多用户的关注，用户只有增强自身的安全防范意识，才不会让别有用心的人有可乘之机。



**要点导航**

- ◎ QQ 攻防
- ◎ 电子邮件攻防

# 6.1 QQ攻防

木马攻击是黑客最喜爱的攻击手段，利用其他的一些载体，木马可以轻松地隐藏在其中。木马的危害性在于它对计算机有着强大的控制和破坏能力，同时还有窃取密码、偷窥重要信息、控制系统操作、进行文件操作等能力，从而达到完全控制目标计算机的目的。

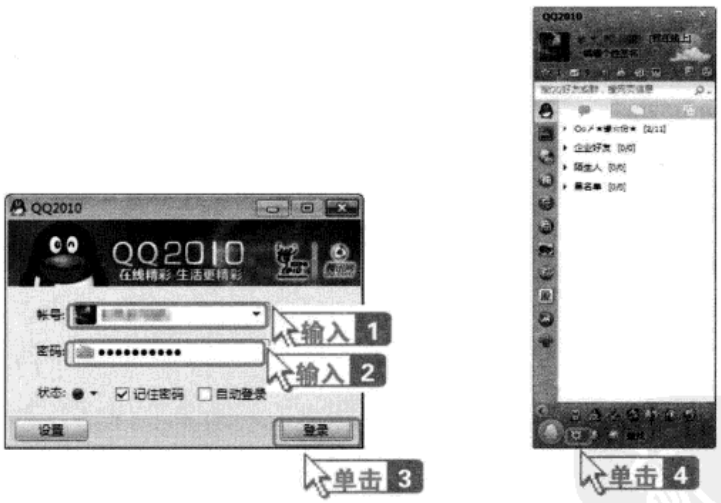
## 6.1.1 保护QQ聊天记录

一般来说，攻击QQ账户主要是指通过某些手段对QQ用户进行恶意侵犯，如私自查看QQ用户的聊天记录、盗取用户QQ号码等，这时就需要用户在退出QQ账户时清除聊天记录。

用户在退出QQ账户后实时清除聊天记录是非常有必要的，这不仅保障了用户聊天记录的安全，也使那些别有用心的人无可乘之机。设置QQ账户在退出时实时清除本机聊天记录的具体步骤如下。

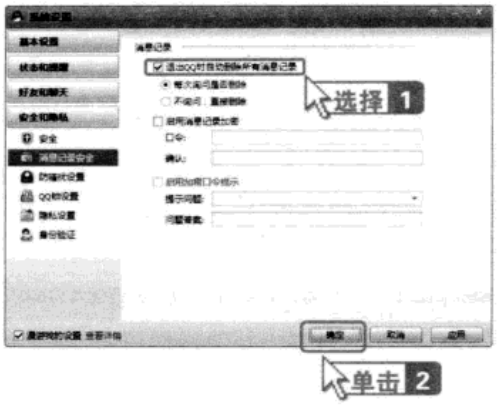
步骤1 打开QQ程序登录界面，输入QQ账号和密码，然后单击 登录 按钮进行登录。

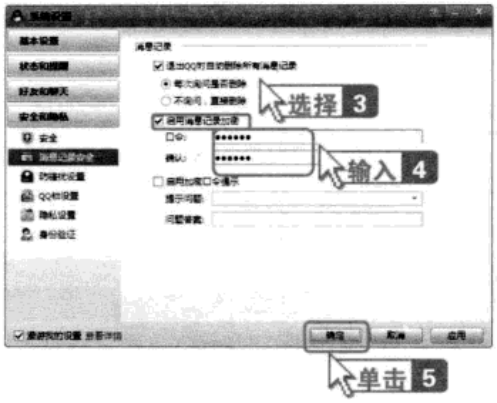
步骤2 登录成功之后，单击程序窗口右下角的按钮。




步骤3 打开【系统设置】对话框，在左侧窗格中选择【安全和隐私】➢【消息记录安全】选项，在右侧窗格中的【消息记录】组合框中选中【退出QQ时自动删除所有消息记录】复选框，然后单击 确定 按钮，即可在退出QQ账号时清除该QQ账号在本机上的所有消息记录。

步骤4 为了保障消息记录的安全，用户还可以选中【消息记录】组合框中的【启用消息记录加密】复选框，然后在【口令】和【确认】文本框中输入密码，最后单击 确定 按钮即可为消息记录加上密码保护。




## 6.1.2 保护QQ密码

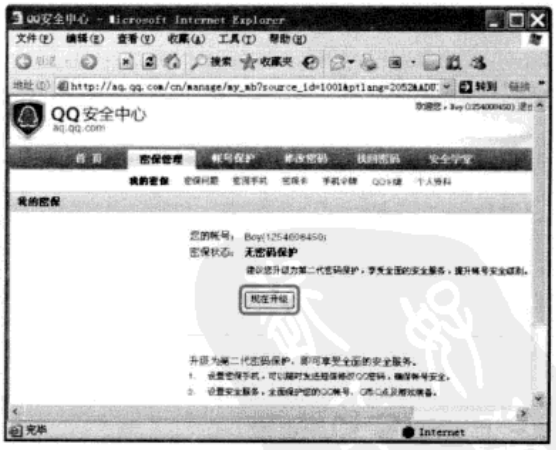
盗取QQ账号密码是黑客攻击QQ用户最常用的手段，为了保障用户QQ账号密码的安全，腾讯公司为QQ账号设计了密码保护功能，用户只有提前申请了密码保护功能，才能够在最短的时间内找回被盗走的QQ账号。

### 1. 设置 QQ 密码保护

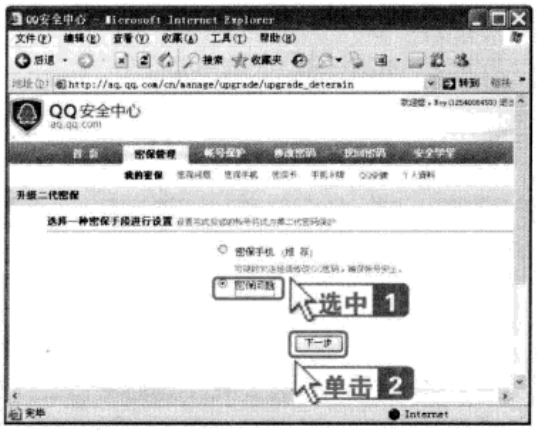
设置QQ账号密码保护，可以在QQ账号被盗时方便地找回自己的QQ账号，下面介绍如何设置QQ账号密码保护。

步骤1 登录QQ账号以后，单击主窗口左下方的按钮，从弹出的快捷菜单中选择【安全中心】➢【申请密码保护】菜单项。

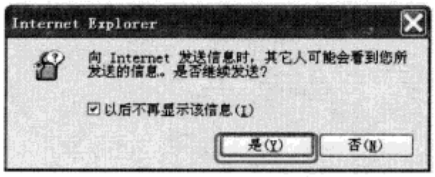

步骤2 弹出【QQ安全中心】网页，切换到【密保管理】选项卡，单击【我的密保】选项中的 现在升级 按钮。



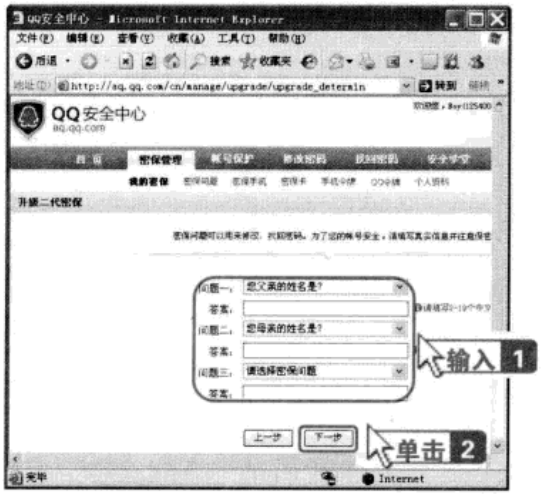

步骤3 在打开的窗口中，用户可以选择一种密保手段进行设置，在这里选中【密保问题】单选钮，然后单击 下一步 按钮。




步骤4 弹出一个提示对话框，单击 是(Y) 按钮即可。

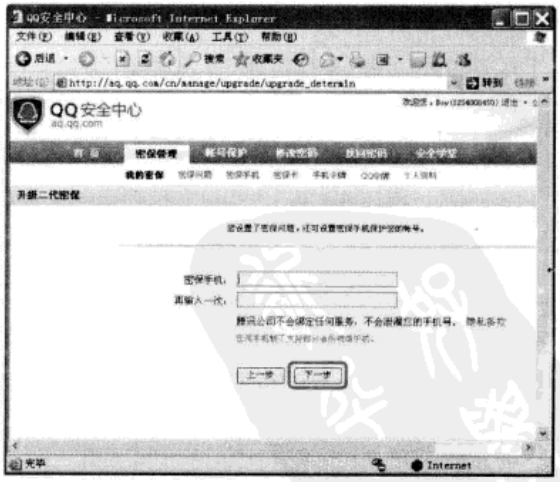



步骤5 进入填写密保阶段，为了账号的安全，用户需填写真实信息并注意保密。在【问题】下拉列表中选择要提问的问题，并在【答案】文本框中填写相应的答案。填写完成后单击 下一步 按钮。




步骤6 在打开的窗口中，用户需对刚刚设置的密保问题依次做出正确回答，以便进行确认。填写完成后单击 下一步 按钮。


步骤7 用户可以在此设置密保手机，设置密保手机后，用户可以通过发送短信及时重设密码，从此不再担心QQ密码遗忘或者丢失。如果用户不想设置密保手机，可以直接单击 下一步 按钮进入下一个阶段。



步骤8 密保问题设置成功，用户现在的密保状态是第二代密码保护，用户可以单击 帐号安全体检 按钮进行账号的安全体检，以便获

得更多的账号安全建议。

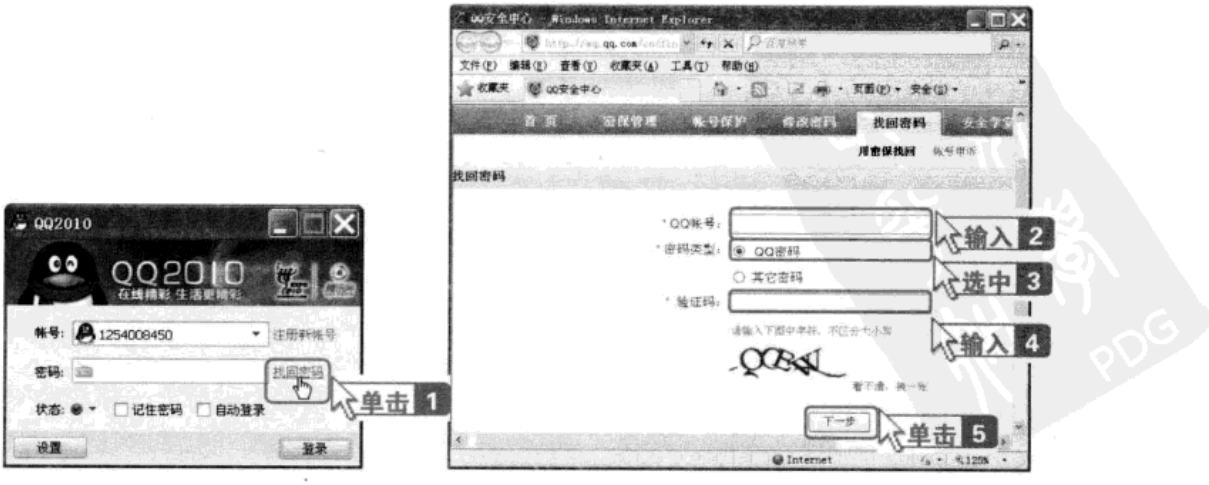

步骤9 在【账号安全体检】窗口中，用户可以看到自己账号当前的安全级别，另外用户可以通过对体检选项的设置来提高账号的安全级别。单击【长期没有使用密保问题】右侧的 立即验证 按钮，验证成功后，账号相应的安全级别也会提高。密保问题设置完成后单击窗口右上角的【退出】链接退出系统，然后关闭【QQ安全中心】网页即可。


## 2. 找回丢失的 QQ 号码

如果用户的QQ账号丢失或者忘记了密码，可以通过获得的密保卡找回自己的QQ账号，具体的操作步骤如下。

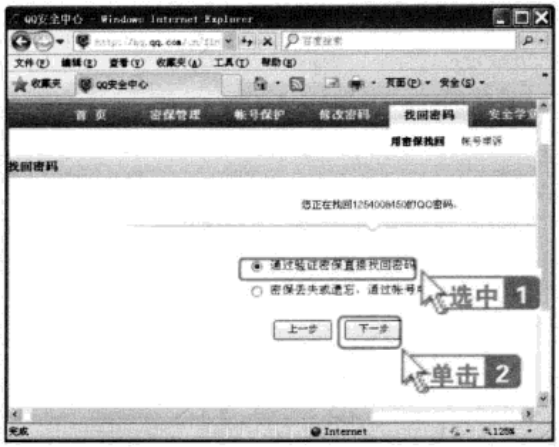
步骤1 运行QQ程序并打开登录窗口，然后单击【密码】文本框右侧的【找回密码】链接。

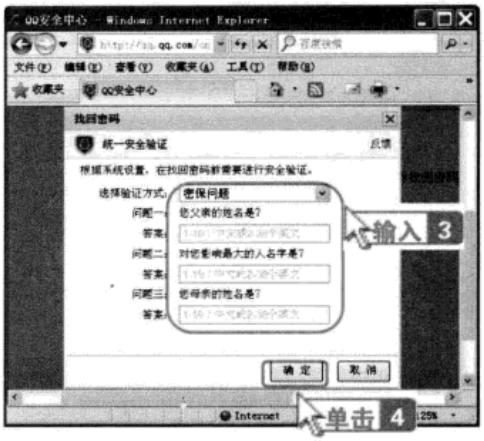
步骤2 打开【QQ安全中心】网页，在【QQ账号】文本框中输入要找回密码的QQ账号，然后选中【QQ密码】单选钮，输入验证码后单击 下一步 按钮。



步骤3 选中【通过验证密保直接找回密码】单选钮，然后单击 下一步 按钮。

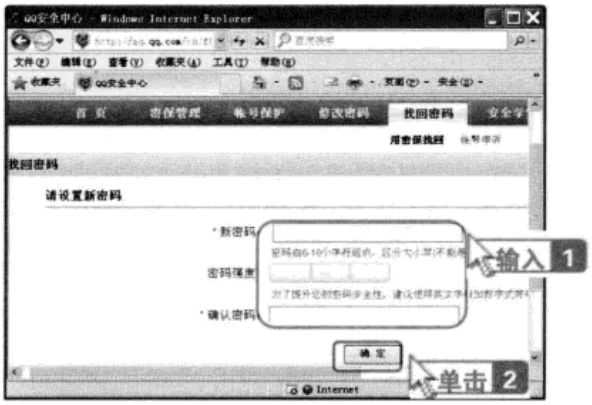
步骤4 在弹出的【找回密码】窗口中正确回答密保问题，然后单击 确 定 按钮。




步骤5 在打开窗口的【请设置新密码】组合框中设置一个新的密码，然后单击 确 定 按钮。

步骤6 新密码设置成功，关闭【QQ安全中心】网页。




## 6.2 电子邮件攻防

电子邮件是目前最常用的通信方式之一，电子邮箱中有可能存放着很多的重要信息，因此电子邮箱也成了黑客的攻击对象，而非法盗取电子邮箱密码就是最常见的一种攻击方式。

### 6.2.1 破解电子邮件的登录密码

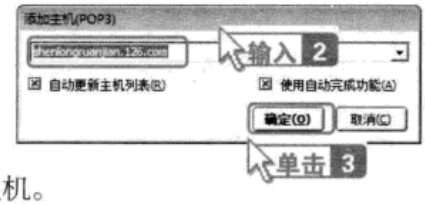
下面介绍如何使用流光软件探测电子邮箱的账号和密码，并暴力破解电子邮箱密码。

## 1. 软件探测

前面已经介绍过流光软件，下面介绍如何使用流光软件探测电子邮箱密码。

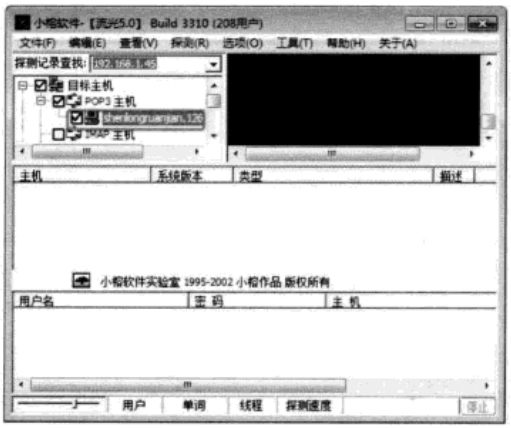
步骤1 首先需要添加一个POP3主机。在流光程序主窗口中选择【目标主机】➢【POP3主机】选项，然后单击鼠标右键，从弹出的快捷菜单中选择【编辑】➢【添加】菜单项。

步骤2 在【添加主机（POP3）】对话框的下拉列表框中添加一个POP3主机，在此以探测126邮箱为例进行介绍。输入“shenlongruanjian.136.com”，然后单击 确定(O) 按钮。

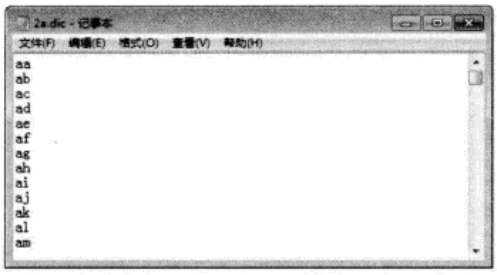

步骤3 返回主界面，此时可以看到添加了一个POP3主机。

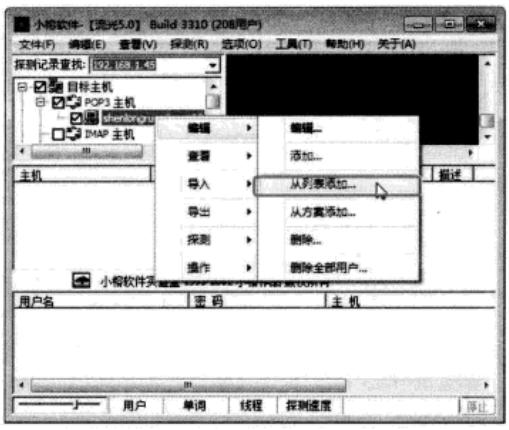
步骤4 接下来需要添加破解账号所需要的用户列表文件。在添加用户列表文件之前可以先对其进行编辑，在流光程序的安装目录中找到要进行编辑的扩展名为“.dic”的用户列表文件，然后单击鼠标右键，从弹出的快捷菜单中选择【打开方式】➢【记事本】菜单项。



步骤5 在以记事本方式打开的用户列表文件中，可以根据需要添加或删除相应的内容，设置完成后保存文件并关闭打开的记事本。

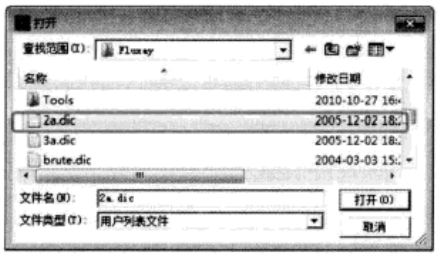
步骤6 在流光程序主窗口的左侧窗格中选中添加的POP3主机，然后单击鼠标右键，从弹出的快捷菜单中选择【编辑】➢【从列表中添加】菜单项。




步骤7 打开【打开】对话框，找到流光文件的安装路径，从中选择编辑过的用户列表文件，然后单击 打开(O) 按钮。

步骤8 此时即可将编辑的用户列表文件添加到POP3主机下。在程序主窗口中选择【探测】➢【简单模式探测】菜单项，程序开始探测，探测完成后弹出探测结果。如果用户列表文件中包含的数据量很大，则需要探测很长时间。



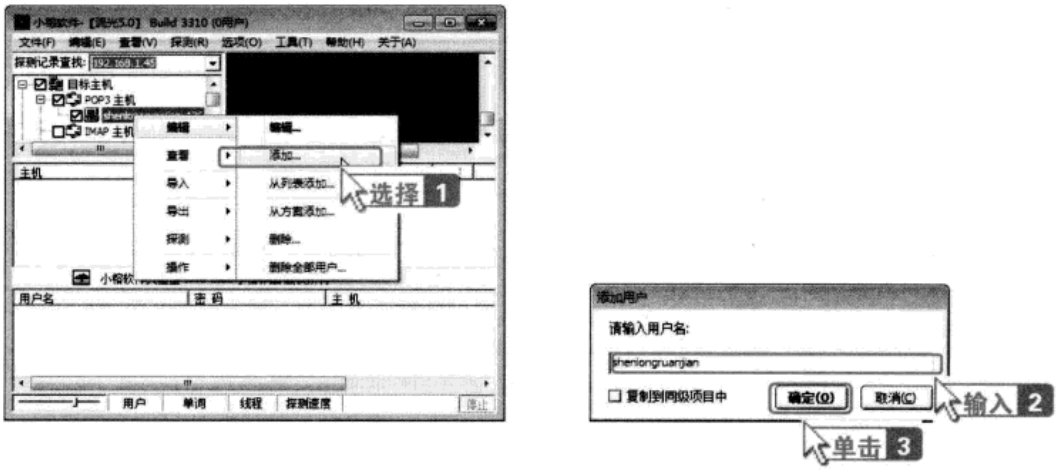


## 2. 暴力破解

如果黑客知道了用户的电子邮箱账号，就会使用流光软件来暴力破解邮箱的密码，如果用户的密码设置得过于简单就很容易被破解。下面介绍如何使用流光软件对已知账号进行密码破解，具体的操作步骤如下。

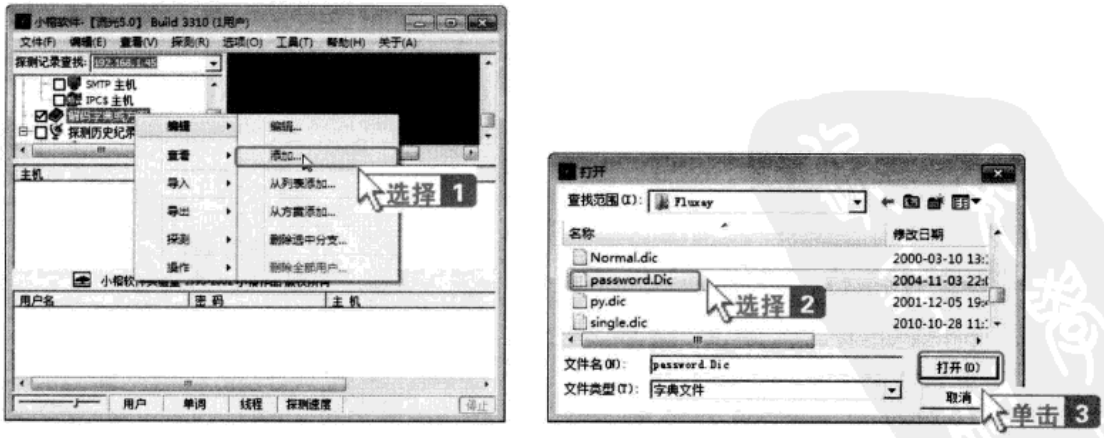
步骤1 添加一个POP3主机，这里仍然以探测名为“shenlongruanjian.126.com”的126主机为例，接下来选中添加的主机，然后单击鼠标右键，从弹出的快捷菜单中选择【编辑】➢【添加】菜单项。

步骤2 在打开的【添加用户】对话框的【输入用户名】文本框中输入已知的126邮箱的用户名，然后单击 确定(O) 按钮，即可在“pop.126.com”主机中看到添加的邮箱用户名。

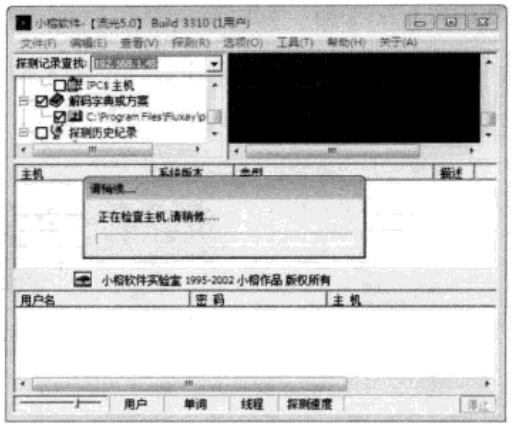



步骤3 添加解码字典。如果用户的邮箱账号密码设置得过于简单，使用流光软件提供的解码字典就可能将其破解。在流光程序的左侧窗格中选择【解码字典或方案】选项，然后单击鼠标右键，从弹出的快捷菜单中选择【编辑】➢【添加】菜单项。

步骤4 弹出【打开】对话框，找到流光程序的安装路径，选择其中的解码字典“password.Dic”，然后单击 打开(O) 按钮（在选择解码字典之前，用户可以根据需要先以记事本方式将其打开进行编辑），即可添加一个解码字典到窗口中。




步骤5 添加完解码字典后，选择【探测】➢【标准模式探测】菜单项，此时流光程序开始破解指定邮箱的登录密码。



## 6.2.2 找回邮箱密码

为了防止一些别有用心的人使用暴力破解软件来盗取邮箱密码，用户最好将邮箱密码设置得复杂一些，例如使用“字母”+“数字”+“特殊字符”的密码组合，而且密码长度最好要大于8位，因为大多数的破解密码软件能够破解的密码长度都在8位以内。

如果用户忘记或丢失了邮箱密码，可以通过邮箱密保来找回丢失的邮箱密码，具体的操作步骤如下（这里以126邮箱账号为例进行介绍）。

步骤1 打开126邮箱账号登录界面，然后单击页面中的【忘记密码？】链接。

步骤2 在打开的页面中列出了几种密码的取回方式，如果用户设置了密码提示，则单击【通过密码提示问题】链接。



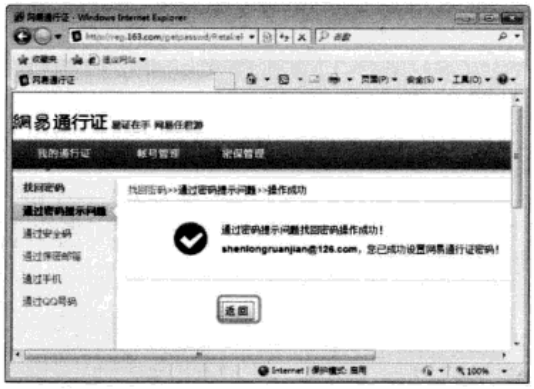
步骤3 在打开的页面中根据提示输入通行证用户名和申请账号时设置的出生日期，然后单击 下一步 按钮。

步骤4 在弹出的页面中根据提示问题在【答案】文本框中输入申请邮箱账号时设置的问题答案，

然后设置新密码，设置完成后单击 完成 按钮。



步骤5 新密码设置成功之后在提示页面中会出现提示信息，此时可以单击 返回 按钮返回126登录页面使用新密码来登录邮箱。




## 6.2.3 防范邮箱炸弹攻击

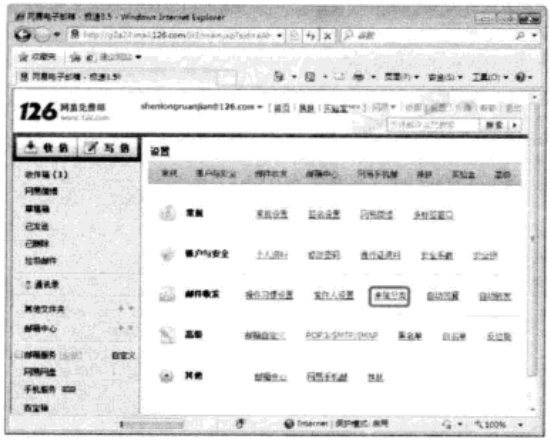
利用邮箱炸弹攻击用户的电子邮箱是黑客使用较为普遍的一种攻击手段，这种攻击手段不仅会干扰用户电子邮件系统的正常使用，甚至还会影响到邮件系统所在服务器系统的安全，造成整个网络系统全部瘫痪，所以邮件炸弹具有一定的危害性。

邮箱炸弹可以消耗大量的网络资源，很容易导致网络塞车，以至于大量的用户不能正常使用邮箱。通常邮箱容量是很有限的，在有限的空间中，如果用户在短时间内收到上千上万封垃圾邮件，邮箱中的空间就会越来越小，以致无法接收新邮件，最终其他用户发来的新邮件就会丢失或者被退回，这时用户的邮箱也就失去了作用。

如果用户的邮箱经常受到邮箱炸弹的攻击，可以采取相应的措施进行防范。在邮箱中设置相应的选项可以大大降低被邮箱炸弹攻击的概率，具体的操作步骤如下（这里以设置126邮箱为例）。

步骤1 打开网页并登录邮箱，单击邮箱页面中的【设置】链接。

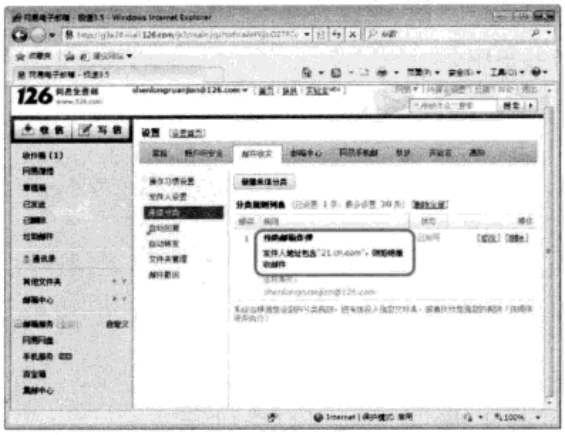

步骤2 在右侧窗格中打开【设置】页面，在右侧窗格中单击【邮件收发】组合框中的【来信分类】链接。



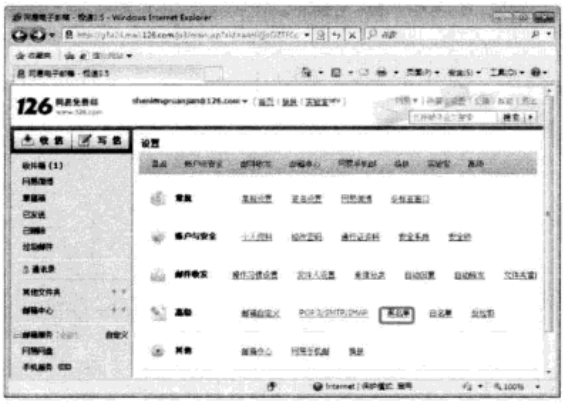
步骤3 打开【来信分类】设置页面，初次使用来信分类功能时，用户需要先创建一个分类规则。单击页面中的 新建来信分类 按钮。

步骤4 进入设置分类规则页面，在【名称】文本框中输入一个规则名称，在【收到邮件时】组合框中根据实际需要进行条件设置，例如要拒收来自21cn邮箱的所有邮件，可以在【收到邮件时：满足以下所有条件】的第一个下拉列表中选择【收件人地址】选项，在第二个下拉列表中选择【包含】选项，并在其下方的文本框中输入“21.cn.com”，接着在【符合上述条件，则执行】下拉列表框中选择【拒收】选项，然后选中【选择账号】单选钮，并选中下方的复选框，设置完成后单击 确定 按钮。

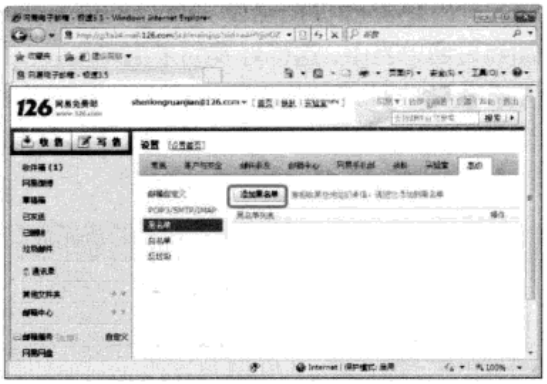
这样就可以过滤掉21cn邮箱发过来的所有邮件了。



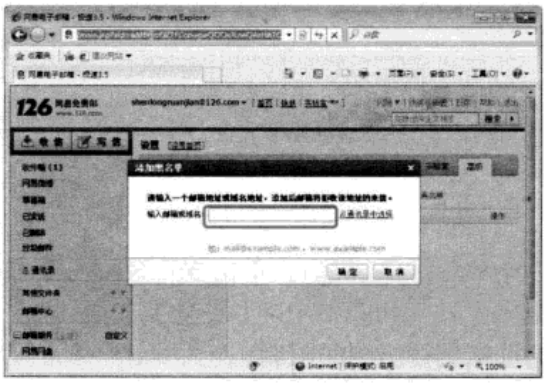
步骤5 如果用户的邮箱经常收到某个陌生邮箱发来的垃圾邮件，可以将该邮箱添加到黑名单中。返回【设置】页面，单击【高级】组合框中的【黑名单】超链接。



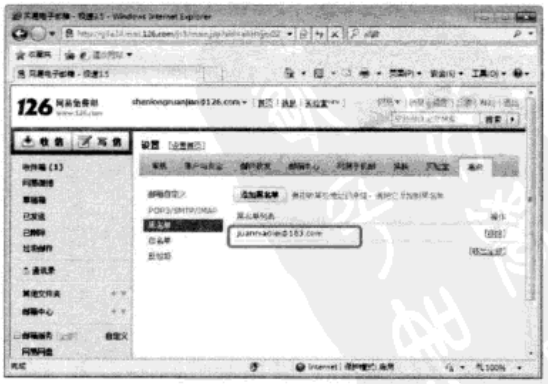
步骤6 进入黑名单设置页面，然后单击 添加黑名单 按钮。



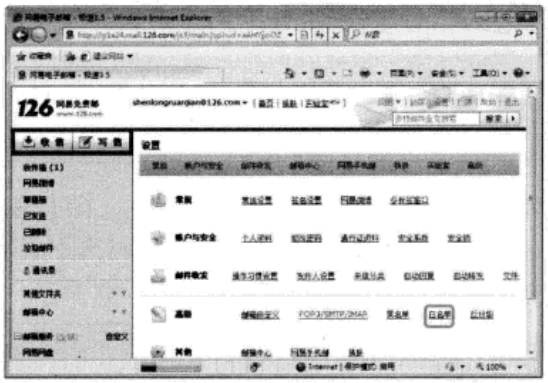
步骤7 弹出【添加黑名单】对话框，在【输入邮箱或域名】文本框中输入要加入黑名单的邮箱地址，然后单击 确 定 按钮。



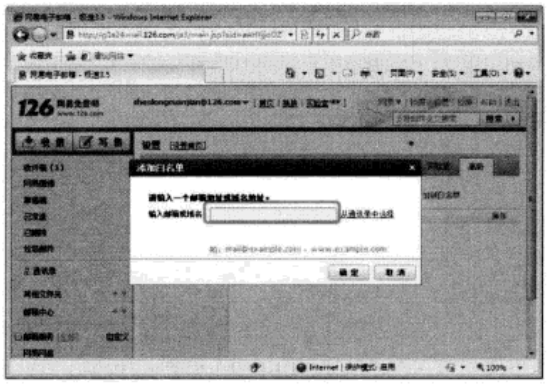
步骤8 设置完成后系统会自动拒收黑名单的来信。



步骤9 用户可以根据需要将自己的好友邮箱添加到白名单当中，这样好友的来信将绕过反垃圾系统直达收件箱。添加白名单的方法非常简单，在【设置】页面的【高级】组合框中单击【白名单】超链接。



步骤10 进入白名单设置页面，单击 添加白名单 按钮，在弹出的【添加白名单】对话框中添加好友邮箱地址，然后单击 确 定 按钮即可将其添加到白名单中。



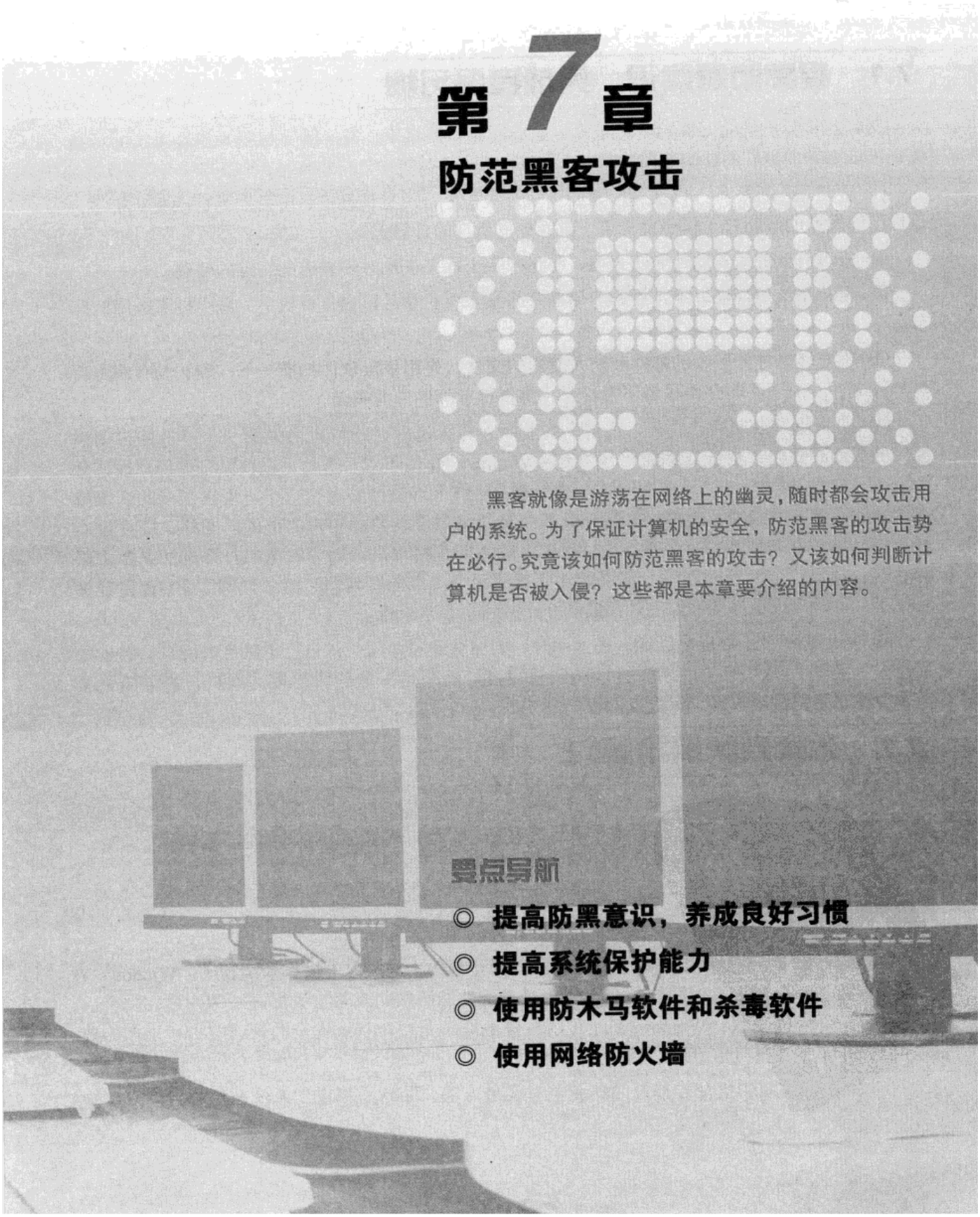
## 新手问题解答

### 如何提高 QQ 文件传输的安全级别

成功登录QQ之后，单击程序窗口右下角的按钮，打开【系统设置】对话框，在左侧窗格中选择【安全和隐私】➢【安全】选项，在右侧窗格的【文件传输】组合框中，可以通过3个选项的选择进行级别的限制。

### 获取账号和密码的方法有哪些

现代社会中，时时刻刻都离不开账号和密码，也就产生了很多获取账号和密码的方法，如口令猜测、暴力破解、网络监听和缓冲区攻击等。



# 第7章 防范黑客攻击

黑客就像是游荡在网络上的幽灵，随时都会攻击用户的系统。为了保证计算机的安全，防范黑客的攻击势在必行。究竟该如何防范黑客的攻击？又该如何判断计算机是否被入侵？这些都是本章要介绍的内容。

**重点导航**

- ◎ 提高防黑意识，养成良好习惯
- ◎ 提高系统保护能力
- ◎ 使用防木马软件和杀毒软件
- ◎ 使用网络防火墙

## 7.1 提高防黑意识，养成良好习惯

良好的计算机使用习惯可以降低计算机感染病毒的概率，减小计算机受到黑客攻击的可能性，所以要养成良好的使用习惯。

(1) 要使用正版软件，以获得厂家的补丁升级程序，并把计算机系统设定为自动更新状态，这样厂商发布的最新补丁程序会在第一时间分发到你的计算机上。

(2) 安装有效的杀毒软件和防火墙，防止因补丁程序未及时安装遭到病毒的侵袭。

(3) 保持系统的简洁，不常用的应用程序尽量不要长期驻留在计算机上，减少排除故障的环节。

(4) 不要轻易打开接收的邮件和别人发送的文件，先用杀毒软件扫描一下，确认没有病毒后再打开文件。对于不明邮件尽量不要打开，防止恶意邮件传播病毒。

(5) 避免使用自动播放功能。有时将U盘插入计算机后，计算机会弹出一个“选择自动播放”的界面，提供“打开文件夹”、“使用Windows Media播放”等若干选项。有些用户往往会图方便，双击其中的“打开文件夹”。殊不知，这样很容易被病毒钻空子。现在很多的病毒就利用这一点篡改U盘的首选项，实现让计算机使用者自己使自己中毒的目的。同样，即便没有开启自动播放功能，用户在使用U盘时也要尽量不要直接双击。较为安全的打开办法是单击鼠标右键，选择“资源管理器”。特别要注意遇到两个“资源管理器”时，说明这个U盘已经被感染了，这时应该选择下面没有加黑的那个，并注意经常杀毒。

(6) 陌生的网页不要轻易尝试。在上网时，要尽量避免访问一些自己不熟悉的网页，特别是跟账户、密码、财产有关的网页，以防账号被盗。特别是一些假冒的银行网页，需要慎之又慎。要在正规的网银页面入口进入网银。

## 7.2 提高系统保护能力

安全是计算机能够正常运行的关键，要想使计算机在安全的环境下运行，就需要了解并掌握设置计算机中安全选项的方法。本章介绍如何通过修复系统漏洞和使用组策略、本地安全策略以及系统日志等系统工具提高系统的防护能力。

### 7.2.1 堵住系统漏洞

Windows操作系统是目前使用最广泛的桌面操作系统，与以前的操作系统相比，Windows 7系统具有更加安全和更加保密的安全特性，对系统性能所做的改善大大提高了用户建立安全、保密和系统环境的系数。Windows 7还可以有效地提高用户对系统安全的管理能力和工作的效率，但Windows 7同样也存在着大量的安全漏洞。

在Windows系统中检测和修复系统漏洞有两种方法，分别是用操作系统自带的自动更新软

件和使用第三方工具。

### 1. 使用 Windows 系统自带的自动更新软件

要使用系统自带的自动更新软件，必须先启用Windows自动更新功能。具体的操作步骤如下。

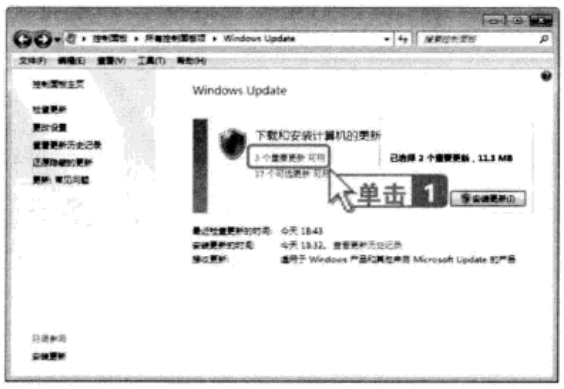
步骤1 选择【开始】➢【控制面板】菜单项，打开【控制面板】窗口，找到并双击【Windows Update】图标。

步骤2 弹出【Windows Update】对话框，在左侧的窗格中单击【检查更新】链接，随即进行检查更新操作。



步骤3 检查完毕后，在右侧的列表框中显示出系统中所存在的漏洞，单击右侧列表框中的 安装更新(I) 按钮即可进行系统漏洞的自动更新。

步骤4 另外，用户也可以单击列表框中的链接进行漏洞的自定义安装。这里单击【3个重要更新 可用】链接，弹出【选择要安装的更新】对话框，然后便可以进行系统漏洞的选择和安装操作。





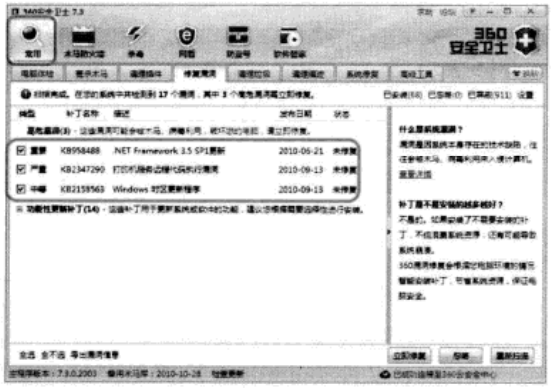
### 2. 使用 360 安全卫士

360安全卫士功能很强大，有查杀流行木马、清理恶评插件、管理应用软件、修复系统漏

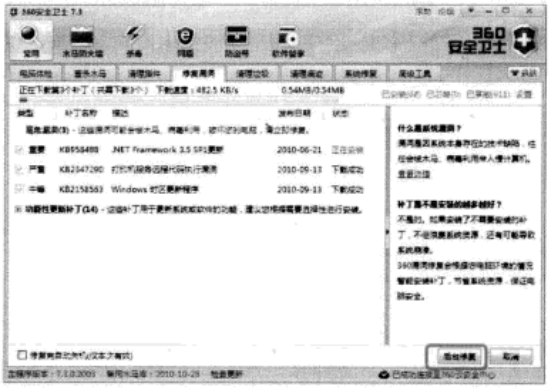
洞、系统全面诊断等功能。这里只介绍360安全卫士的修复系统漏洞功能。具体的操作步骤如下。

步骤1 启动360安全卫士，打开其主界面。

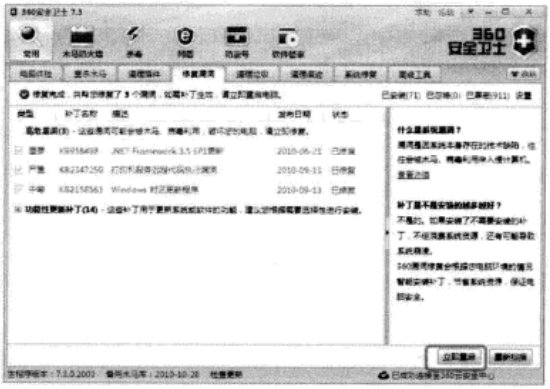
步骤2 单击 按钮，并切换到【修复漏洞】选项卡，此时软件会自动检测系统漏洞。



步骤3 检测完成后，选中要修复的系统漏洞，然后单击 后台修复 按钮即可。



步骤4 修复完成后单击 立即重启 按钮即可。



## 7.2.2 保护注册表安全

注册表是Windows操作系统中极其重要的组成部分，如果注册表被破坏，会导致计算机中的许多程序和功能不能使用，甚至造成操作系统的瘫痪。为了防止注册表被破坏，用户有必要掌握注册表安全管理的方法。

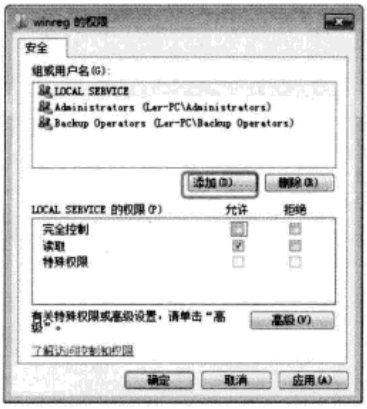
### 1. 限制远程访问

注册表的远程访问功能是微软在Windows中提供的一项旨在方便用户管理远程计算机上的注册表的功能。使用此项功能，用户可以很方便地对远程计算机上的注册表进行管理和维护，但如果这项功能被一些别有用心的人利用的话，很可能会给用户造成一些不必要的损失。下面介绍一些注册表远程访问管理的知识。

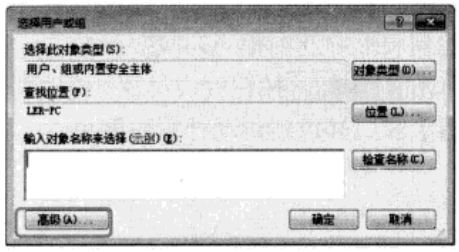
在注册表中有一些关键的注册表项是不能被修改的，用户可以通过修改注册表来限制对这些敏感注册表项的访问。具体的操作步骤如下。

步骤1 按照前面介绍的方法打开【注册表编辑器】窗口，然后在左侧的列表框中找到HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winre注册表项，在该注册表项上单击鼠标右键，从弹出的快捷菜单中选择【权限】菜单项。

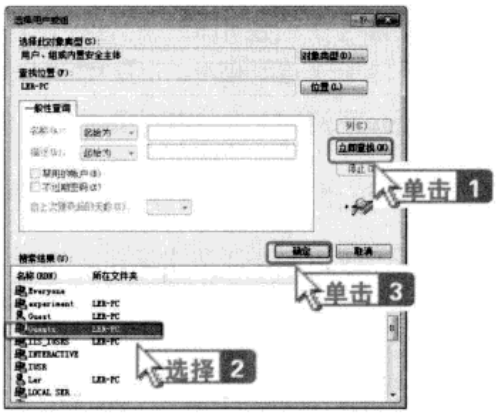
步骤2 打开【winreg的权限】对话框，单击 添加(D)... 按钮。



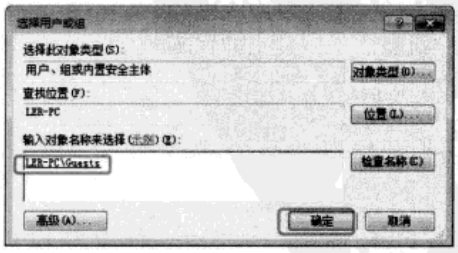

步骤3 弹出【选择用户或组】对话框，单击 高级(A)... 按钮。



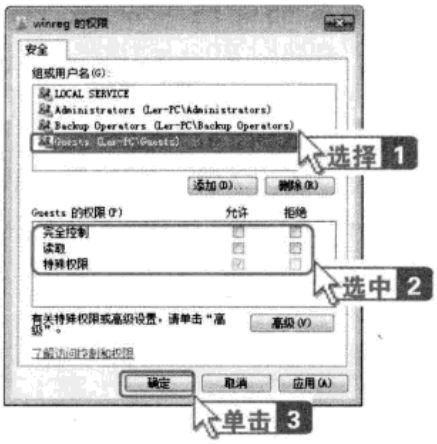

步骤4 弹出其高级选择面板，单击 立即查找(N) 按钮，Windows将会查找计算机中的所有用户或组并将结果显示在下面的列表框中，选中想要被设置权限的用户或组，然后单击 确定 按钮。




步骤5 返回【选择用户或组】对话框，可以看到选择的用户或组添加到了【输入对象名称来选择（示例）】列表框中，然后单击 确定 按钮。



步骤6 返回【winreg的权限】对话框，可以发现用户选择的用户名称显示在【组或用户名称】列表框中。选中想要设置权限的用户名称，并在下面的列表框中选中相应的权限后面的复选框，接着单击 确定 按钮完成设置。退出【注册表编辑器】窗口并重新启动计算机即可。



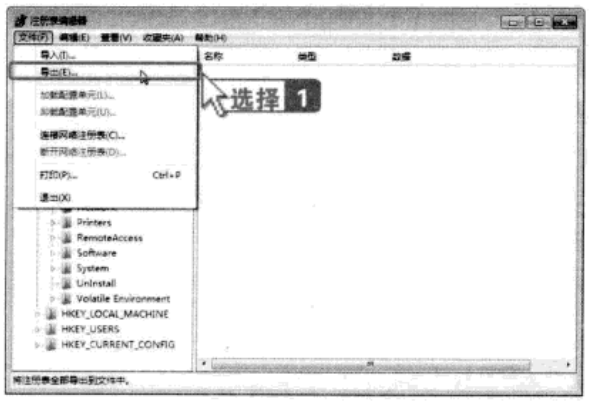

## 2. 备份与还原注册表

注册表在Windows操作系统中的地位非同一般，它集中了与软件和硬件相关的配置和状态信息，以及与用户使用相关的各种设置信息。为了防止注册表损坏，用户需要对注册表进行备份，一旦注册表遭到破坏，用户便可以使用已经备份的注册表进行还原操作。

下面介绍两种备份注册表的方法。

### 使用注册表编辑器中自带的导出功能备份注册表

打开【注册表编辑器】窗口，选择【文件】➢【导出】菜单项，弹出【导出注册表文件】对话框，从中设置注册表备份文件保存的路径、名称、保存类型以及导出范围等。在【导出范围】组合框中，用户可以选择是全部导出还是导出相应的分支。如果选中【全部】单选钮，则可以将整个计算机的注册表进行备份；如果选中【所选分支】单选钮，则可以进行单个分支注册表的备份。设置好导出注册表备份的选项以后，单击 保存(S) 按钮，完成相应注册表的导出备份操作。




### 手动备份注册表

在Windows 7中，系统配置文件一般保存在系统盘中WINDOWS/system32/config目录下的Config文件夹中，主要包括SAM、system、software和default等几个无后缀的文件以及与之相对应的log文件。用户配置文件保存在Windows 7系统盘的Users文件夹中，主要包括Ntuser.dat和与之对应的log文件。

手动备份注册表时，用户只需将上面所提到的文件复制到其他磁盘分区的文件夹中即可。如果用户安装了多个操作系统，也可以在其他操作系统中备份这些文件。

当然，除了上面介绍的备份注册表的方法之外，用户还可以借助一些软件来实现注册表的备份操作，例如，使用Windows优化大师或超级兔子进行备份等。

备份注册表以后，便可以对注册表进行修改而不用担心注册表损坏。因为一旦注册表被损坏，用户可以使用已备份的注册表进行还原，这样注册表就又会恢复到以前的正常状态。

还原注册表的操作很简单，按照前面的方法打开【注册表编辑器】窗口，然后选择【文件】➤【导入】菜单项，打开【导入注册表文件】对话框，从中找到并选中想要导入的注册表备份文件，然后单击 打开(O) 按钮即可完成备份注册表的导入。


## 7.2.3 设置组策略

组策略就是指基于组的策略，它以Windows中的一个MMC管理单元的形式存在，通过它可以帮助系统管理员针对整个计算机或特定的用户来设置多种配置，如桌面配置和安全配置等。

### 1. 开机策略

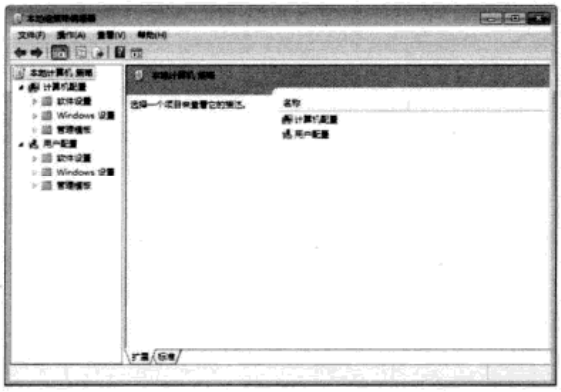
用户可以使用组策略来对开机进行设置，以使自己的计算机和隐私更加安全可靠。

## 设置账户锁定策略

在默认情况下，用户在登录界面中可以有多次输入无效用户账户和密码的机会，而这也为一些使用字典攻击的网络攻击者提供了快速破解用户账户和密码的机会，从而给用户的利益带来损害。为了解决这一问题，用户可以使用组策略来设置账户锁定策略，以将非法用户阻挡于系统之外。

系统内置的Administrator账户即超级管理员账户不会因为账户锁定策略的设置而被锁定，然而当使用远程桌面连接时，会因为账户锁定策略的设置而使得超级管理员账户在限定的时间内无法使用远程桌面。用户需要知道，超级管理员账户的本地登录是永远被允许的。设置账户锁定策略的操作步骤如下。

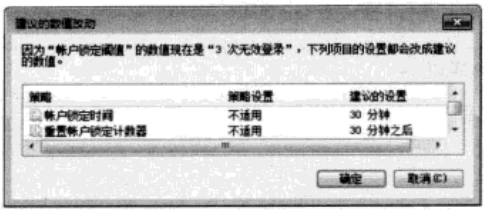
步骤1 选择【开始】➢【运行】菜单项，打开【运行】对话框，在【打开】下拉列表中输入“gpedit.msc”命令并按下【Enter】键，打开【本地组策略编辑器】窗口。



步骤2 在该窗口中依次展开【本地计算机 策略】➢【计算机配置】➢【Windows设置】➢【安全设置】➢【账户策略】➢【账户锁定策略】选项，用户可以在右侧窗格中看到3个账户锁定策略选项，分别为【账户锁定时间】、【账户锁定阈值】和【重置账户锁定计数器】。用鼠标右键单击相应的选项，从弹出的快捷菜单中选择【属性】菜单项（或者直接在相应的选项上双击），这里双击【账户锁定阈值】选项。

步骤3 弹出【账户锁定阈值 属性】对话框，默认情况下，账户为不锁定状态，用户可以设置无效登录的次数（下限为0，上限为999次）。用户可以根据自己的实际情况进行设置，例如，此处设置为可以输入3次无效输入，然后单击 确定 按钮。

步骤4 打开【建议的数值改动】对话框，单击 确定 按钮。




步骤5 返回组策略主窗口，可以看到其他两个策略选项的数值会自动被设置为被建议的数值。如果用户不想使用系统建议的数值，可以单击 取消(C) 按钮，再在【本地组策略编辑器】窗口的右侧窗格中双击其他两个策略选项，然后在打开的相应的属性对话框中设置想要设置成的数值即可（其上限数值均为99999，单位为s）。

## 设置密码锁定策略

密码是用户登录到系统的凭证，只有输入了正确的密码，用户才能正常进入系统中。为了防止其他用户进入系统，用户可以通过设置密码策略来加强系统的安全性。

设置密码锁定策略在一定程度上能够防止其他用户登录自己的计算机，具体的操作步骤如下。

步骤1 在【本地组策略编辑器】窗口中依次展开【本地计算机 策略】➢【计算机配置】➢【Windows设置】➢【安全设置】➢【账户策略】➢【密码策略】项，然后在右侧窗格中双击相应的密码策略选项，打开对应的属性对话框，这里双击【密码最长使用期限】密码策略选项。

步骤2 打开【密码最长存留期 属性】对话框，用户可以设置相应的密码最长存留期的数值。默认情况下该数值为42。用户可以直接在【密码过期时间】微调框中输入数值，也可以单击微调按钮来调节相应的数值，设置完成后单击 确定 按钮即可。

为了能更好地设置密码，下表列出了【密码必须符合复杂性要求】、【密码长度最小值】、【密码最短使用期】、【密码最长使用期】、【强制密码历史】和【用可还原的加密来储存密码】这6个密码策略的功能说明。

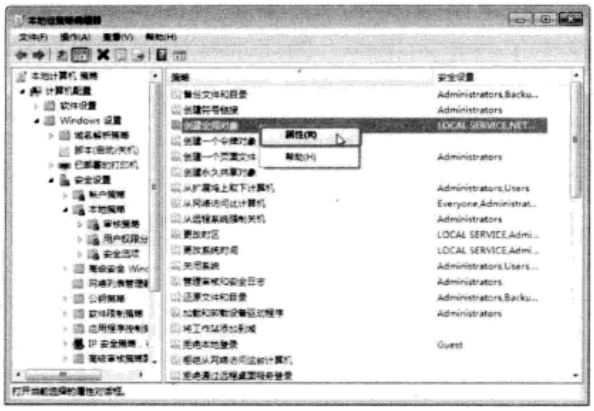
| 密码策略 | 功能说明 |
| --- | --- |
| 密码必须符合复杂性要求 | 确定密码是否必须符合复杂性要求。如果启动该策略，则密码必须满足以下最低要求：<br>(1) 不包含全部或部分的用户账号名<br>(2) 长度至少为 6 个字符<br>(3) 包含来自以下 4 个类别中的 3 个字符：<br>① 英文大/小写字母（A～Z/a～z）<br>② 10 个基本数字（0～9）<br>③ 非字母字符（如!、@、#、$等）<br>更改或创建密码时，会强制执行复杂性要求 |
| 密码长度最小值 | 确定用户账号的密码可以包含的最少字符个数，可以设置为 1～14 个字符的值，或者通过将字符设置为 0，以设置为不需要密码 |
| 密码最短使用期 | 确定用户可以更改密码之前必须使用该密码的时间（单位为天）。可以设置为 1～999 的某个数值，或者通过将数值设置为 0，允许立即更改密码 |
| 密码最长使用期 | 确定系统要求用户更改密码之前可以使用该密码的时间（单位为天）。可以将密码设置为 1～999 的某个数值后过期，或者通过将数值设置为 0 以指定该密码永不过期 |
| 强制密码历史 | 确定在重新使用旧密码前，必须与某一个用户账户相关的唯一新密码个数。该值必须为 0～24。该策略通过确保旧密码不能继续使用，从而使用户能够增强安全性 |
| 用可还原的加密来储存密码 | 如果应用程序使用了要求知道用户密码才能进行身份验证的协议，则该策略可以对它提供支持。使用可逆加密存储密码和存储密码的明文版本本质上是相同的。因此，除非应用程序有比保护密码信息更重要的要求，否则不必启用该策略 |

## 设置用户权限

通过组策略来设置计算机用户权限，在不同的权限下，不同的用户可以进行不同的操作。设置用户权限的方法有两种，一种是通过【创建全局对象】中的指派用户权限来设置，另一种是通过【绕过遍历检查】中的指派用户权限来设置。

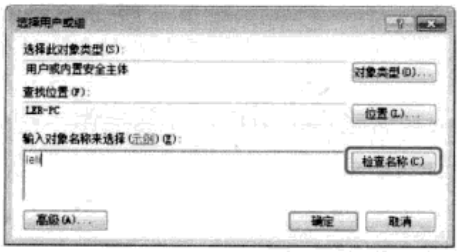
(1) 通过【创建全局对象】设置用户权限

步骤1 选择【开始】➢【运行】菜单项，打开【运行】对话框，在【打开】下拉列表中输入“gpedit.msc”命令，并按下【Enter】键，打开【本地组策略编辑器】窗口，在该窗口中依次展开【本地计算机 策略】➢【计算机配置】➢【Windows设置】➢【安全设置】➢【本地策略】➢【用户权限分配】选项，然后在右侧窗口中的【创建全局对象】选项上单击鼠标右键，从弹出的快捷菜单中选择【属性】菜单项。



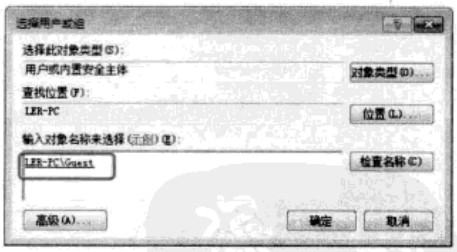
步骤2 打开【创建全局对象 属性】对话框，单击 添加用户或组(U)... 按钮。


步骤3 打开【选择用户或组】对话框，在【输入对象名称来选择（示例）】文本框中输入一个对象名称，然后单击右边的 检查名称(C) 按钮来检查该名称是否存在。




步骤4 如果用户不清楚想要添加的用户或组的名称，可以单击 高级(A)... 按钮，进入高级选择界面。然后单击 立即查找(N) 按钮，Windows将进行用户或组的搜索，搜索完成后选中想要添加的对象，然后单击 确定 按钮。


步骤5 返回【选择用户或组】对话框，此时可以发现选中的用户或组被添加到了【输入对象名称来选择（示例）】文本框中，单击 确定 按钮。




步骤6 返回【创建全局对象 属性】对话框，可以发现相应的用户或组的名称被添加到了列表框中，这样就将全局的权限赋予了该特定用户。

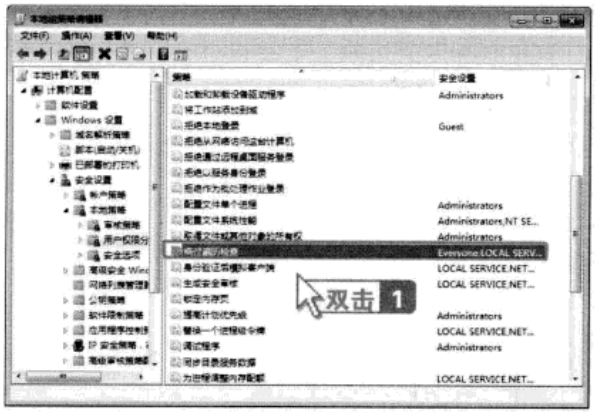

在上述操作中，用户所设置的将全局权限赋予了特定的用户，即所选择的用户拥有和Administrator一样的权限。如果用户想要将某个用户的权限加以限制的话，可以在【创建全局对象 属性】对话框的列表框中选中该用户名称，然后单击 删除(R) 按钮即可。

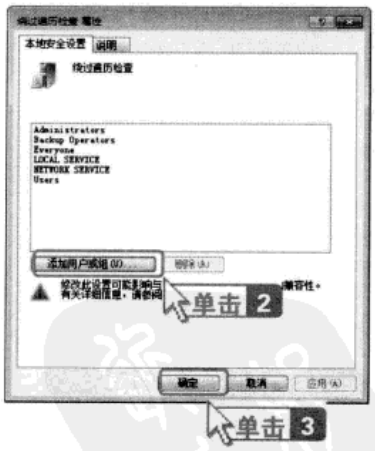
(2) 通过【绕过遍历检查】设置用户权限

用户除了可以在【创建全局对象 属性】对话框中指派用户权限以外，还可以在【绕过遍历检查 属性】对话框中指派用户权限。

步骤1 在前面打开的【本地组策略编辑器】窗口的右侧窗格中找到【绕过遍历检查】选项并双击。

步骤2 打开【绕过遍历检查 属性】对话框，单击 添加用户或组(U)... 按钮之后便可以进行与在【创建全局对象 属性】对话框中指派用户权限一样的操作。添加完成以后，单击 确定 按钮即可。




## 更改系统默认的管理员账户

默认情况下，系统管理员账户的名称为Administrator。该账户是用户在安装操作系统时预置的账户，并不需要用户创建。如果用户在安装操作系统时没有设置该账户的密码，则只需要单击该账户即可进入系统。

Administrator账户的存在虽然方便了用户在忘记密码时登录到系统中，但也为系统的安全带来了风险。因为这个名称是Windows默认的，所以网络攻击者往往会利用用户计算机系统中的

漏洞而使用该账户登录到用户的计算机，从而做出一些侵害用户权益的行为。

为了避免这种情况的发生，用户可以为Administrator账户设置一个通用的密码，或者更改名称，让网络攻击者识别不出哪个是超级管理员账户。更改Administrator账户的具体步骤如下。

步骤1 打开【组策略】窗口，依次展开【本地计算机 策略】➢【计算机配置】➢【Windows设置】➢【安全设置】➢【本地策略】➢【安全选项】项，然后在右侧窗格中找到并双击【账户：重命名系统管理员账户】选项。

步骤2 打开【账户：重命名系统管理账户 属性】对话框，在【账户：重命名系统管理员账户】文本框中输入想要命名的账户名称，然后单击 确定 按钮即可。



### 2. 安全设置

使用组策略可以进行安全设置。

## 禁用 Guest 账户

系统中的Guest账户是为了方便其他的访问者而设置的，但是，这个账户的存在往往也会成为非法用户入侵用户计算机的“方便之门”。如果用户不使用Guest账户，最好是将其禁用，以保证计算机系统的安全。禁用Guest账户有通过【控制面板】和【本地组策略编辑器】来进行操作两种方法。

下面介绍通过【控制面板】来禁用Guest账户的具体步骤。

步骤1 打开【控制面板】窗口，在其中找到并双击【用户账户】选项。

步骤2 弹出【用户账户】窗口，单击【管理其他账户】链接。



步骤3 弹出【管理账户】窗口，在【选择希望更改的账户】组合框中单击【Guest】按钮。

步骤4 弹出【更改来宾选项】窗口，单击【关闭来宾账户】链接即可。



下面介绍通过【本地组策略编辑器】来禁用Guest账户的具体步骤。

步骤1 打开【本地组策略编辑器】窗口，在左侧窗格中依次展开【本地计算机 策略】➤【计算机配置】➤【Windows设置】➤【安全设置】➤【本地策略】➤【安全选项】选项，在右侧的窗格中找到并双击【账户：来宾账户状态】选项。

步骤2 弹出【账户：来宾账户状态 属性】对话框，选中【已禁用】单选钮，然后单击 确定 按钮即可。

## 在局域网中，禁用 Guest 账户是否会影响打印机和文件的共享？

在局域网中，禁用Guest账户后，就无法进行文件和打印机的共享。如果用户需要进行共享，可以启用Guest账户，但出于安全考虑，最好是给Guest账户设置密码。



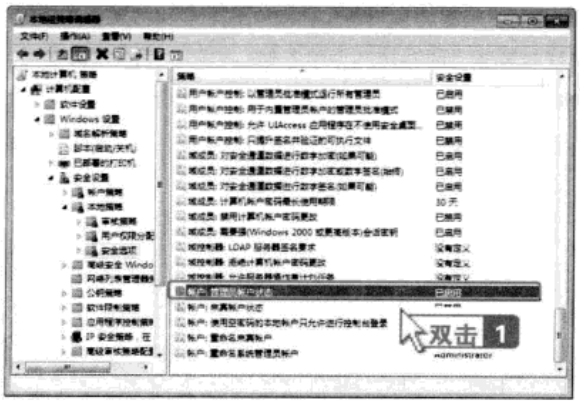
另外，用户还可以像重命名Administrator一样，也可以重命名Guest账户。

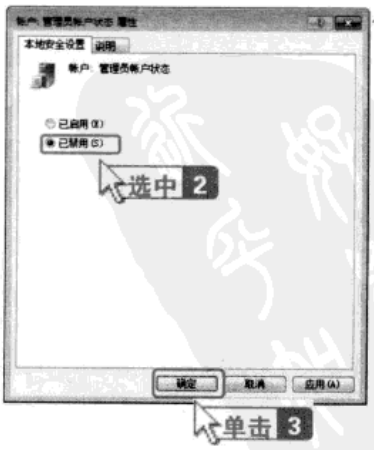
## 禁用 Administrator 账户

为了更好地保护计算机系统，用户有必要创建一个拥有与Administrator账户一样权限的账户，这样便可以将Administrator账户禁用，从而杜绝安全漏洞。禁用Administrator账户可以在组策略中进行，具体的操作步骤如下。

步骤1 打开【本地组策略编辑器】窗口，在左侧窗格中依次展开【本地计算机 策略】➢【计算机配置】➢【Windows设置】➢【安全设置】➢【本地策略】➢【安全选项】选项，在右侧的窗格中找到并双击【账户：管理员账户状态】选项。

步骤2 弹出【账户：管理员账户状态 属性】对话框，选中【已禁用】单选钮，然后单击 确定 按钮即可。



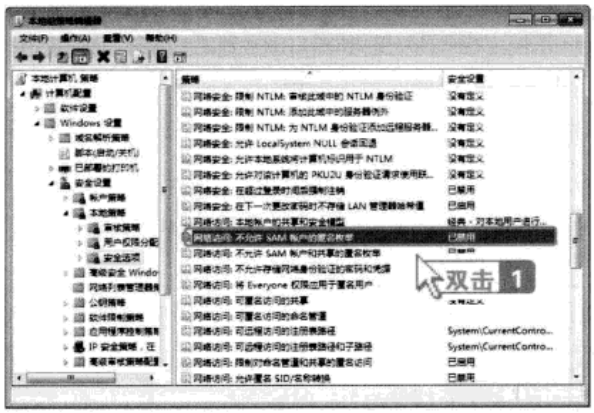



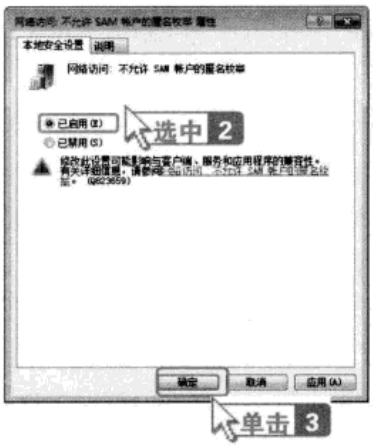
## 不允许 SAM 账户匿名枚举

SAM是Security Account Manager的缩写，意思是安全账户管理器。在SAM文件中记录了计算机中所有用户账户的账户名称和密码，这样在登录时用户可以使用不同的用户名登录到计算机系统中。

步骤1 打开【本地组策略编辑器】窗口，在左侧窗格中依次展开【本地计算机 策略】➢【计算机配置】➢【Windows设置】➢【安全设置】➢【本地策略】➢【安全选项】选项，在右侧的窗格中找到并双击【网络访问：不允许SAM账户的匿名枚举】选项。

步骤2 弹出【网络访问：不允许SAM账户的匿名枚举 属性】对话框，选中【已启用】单选钮，然后单击 确定 按钮即可。




### 为什么不允许 SAM 账户和共享匿名枚举?

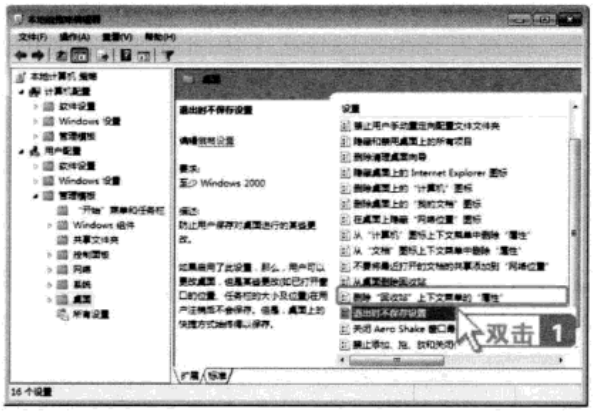
“网络访问：不允许SAM账户和共享的匿名枚举”设置确定是否允许匿名枚举安全账户管理器(SAM)账户和共享。Windows允许匿名用户执行某些活动，如枚举域账户和网络共享的名称。例如，当管理员希望向不维护双向信任的受信任域中的多个用户授予访问权限时，这会非常方便。如果用户不希望允许匿名枚举SAM账户和共享，则启用此设置。但是，即使启用了此设置，匿名用户仍将能够访问具有某些权限（显然包括特殊的内置组ANONYMOUS LOGON）的任何资源。

## 禁止更改桌面设置

用户可以通过修改组策略中的【桌面】选项来禁止更改计算机桌面的设置。具体的操作步骤如下。

步骤1 打开【本地组策略编辑器】窗口，在左侧窗格中依次展开【本地计算机 策略】➢【用户配置】➢【管理模板】➢【桌面】选项，在右侧的窗格中找到并双击【退出时不保存设置】选项。

步骤2 弹出【退出时不保存设置】对话框，选中【已启用】单选钮，然后单击 确定 按钮即可。



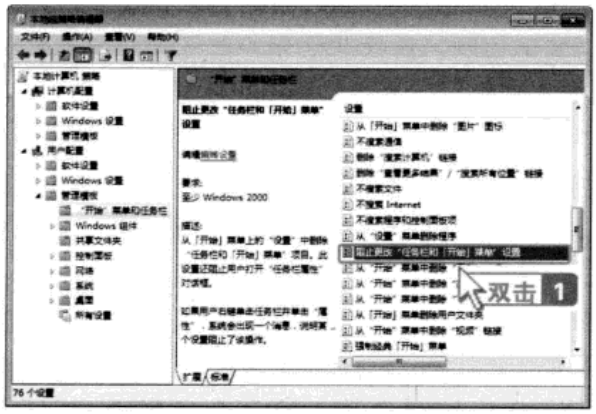


## 禁止更改【开始】菜单和任务栏

通过组策略中的【任务栏和开始菜单】选项可以禁止其他用户更改【开始】菜单和任务栏。具体的操作步骤如下。

步骤1 打开【本地组策略编辑器】窗口，在左侧窗格中依次展开【本地计算机 策略】➢【用户配置】➢【管理模板】➢【“开始”菜单和任务栏】选项，在右侧的窗格中找到并双击【阻止更改“任务栏和「开始」菜单”设置】选项。

步骤2 弹出【阻止更改“任务栏和「开始」菜单”设置】窗口，选中【已启用】单选钮，然后单击 确定 按钮即可。

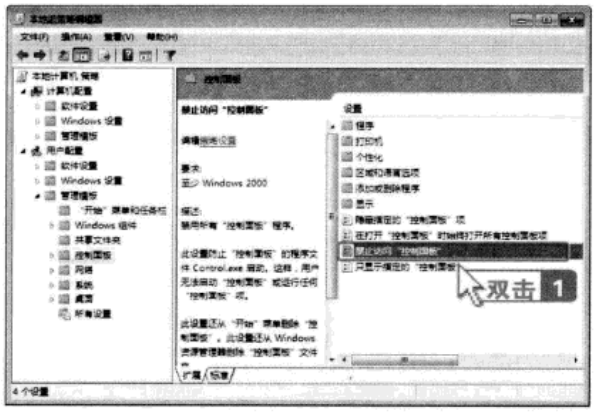


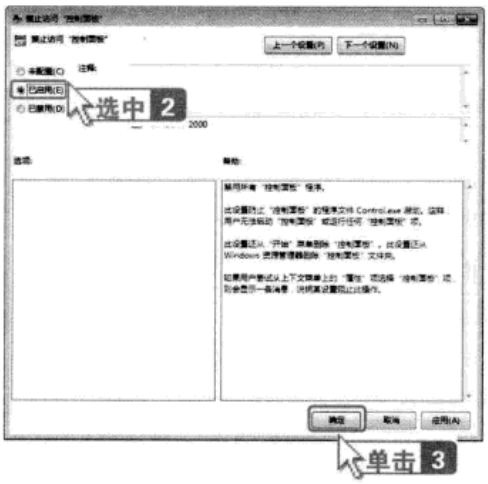

## 禁止访问控制面板

通过访问控制面板可以添加和删除程序、更改用户账号和密码以及设置文件夹选项等，为了防止其他用户通过访问控制面板进行上述操作，通过设置组策略中的【控制面板】选项可以禁止访问控制面板。具体的操作步骤如下。

步骤1 打开【本地组策略编辑器】窗口，在左侧窗格中依次展开【本地计算机 策略】➢【用户配置】➢【管理模板】➢【控制面板】选项，在右侧的窗格中找到并双击【禁止访问“控制面板”】选项。

步骤2 弹出【禁止访问“控制面板”】窗口，选中【已启用】单选钮，然后单击 确定 按钮即可。




## 禁止访问指定的磁盘驱动器

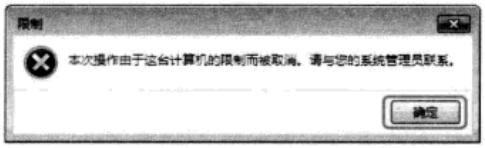
用户可以将一些重要的磁盘驱动器设置为禁止访问，这样非法用户就无法访问这些驱动器，从而也就无法窃取存储在这些驱动器中的敏感文件了。使用组策略可以禁止访问这些指定的磁盘驱动器，具体的操作步骤如下。

步骤1 打开【本地组策略编辑器】窗口，在左侧窗格中依次展开【本地计算机 策略】➢【用户配置】➢【管理模板】➢【Windows组件】➢【Windows资源管理器】选项，在右侧的窗格中找到并双击【防止从“我的电脑”访问驱动器】选项。

步骤2 弹出【防止从“我的电脑”访问驱动器】窗口，选中【已启用】单选钮，此时【选择下列组合中的一个】下拉列表被激活，单击【选择下列组合中的一个】右侧的▾按钮，在弹出的下拉列表中选择想要禁止访问的驱动器，这里选择【只限制D驱动器】选项，然后单击 确定 按钮即可。



步骤3 当进行上述操作以后，双击D盘时，系统会打开【限制】对话框，提示用户操作已被取消。




## 禁止部分应用程序

在公用的计算机中，为了确保其他人不使用自己的某些应用程序，用户可以禁用部分应用程序。禁用部分应用程序的方法有好几种，在这里主要介绍以下两种禁用方法。

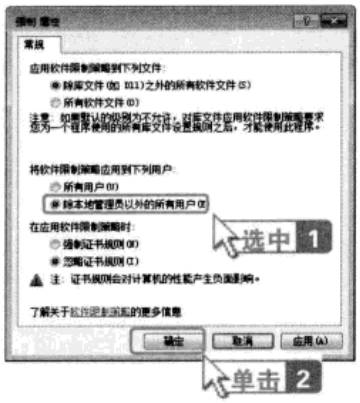
(1) 通过【软件限制策略】设置

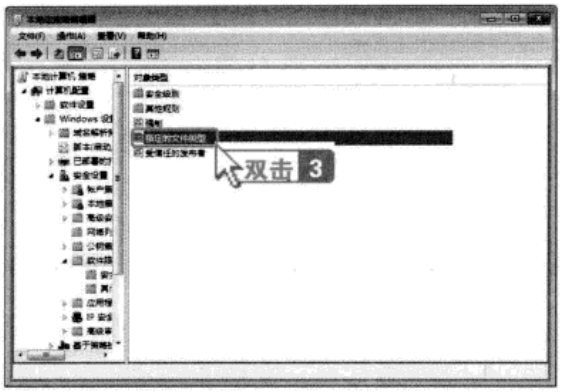
步骤1 打开【本地组策略编辑器】窗口，依次展开【本地计算机 策略】➢【计算机配置】➢【Windows 设置】➢【安全设置】➢【软件限制策略】选项，然后选择【操作】➢【创建新的策略】菜单项。

步骤2 在右侧窗格中的【强制】选项上单击鼠标右键，从弹出的快捷菜单中选择【属性】菜单项（或双击【强制】选项）。


步骤3 打开【强制 属性】对话框，在【将软件限制策略应用到下列用户】组合框中选中【除本地管理员以外的所有用户】单选钮，然后单击 确定 按钮。

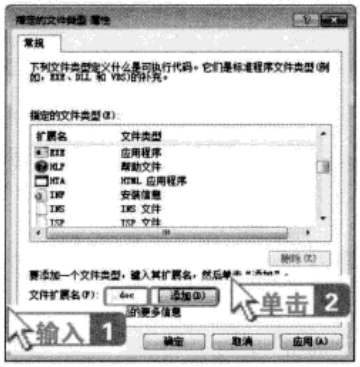
步骤4 返回【本地组策略编辑器】窗口，双击【指派的文件类型】选项。

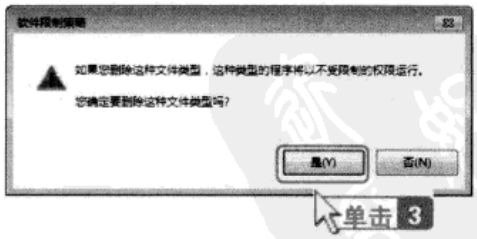



步骤5 打开【指派的文件类型 属性】对话框，在【指定的文件类型】列表框中显示的是被定义为可执行代码文件的扩展名。用户可以在【文件扩展名】列表框中输入想要添加到【指定的文件类型】列表框中的文件扩展名（例如添加扩展名为.doc的文件），然后单击 添加(D) 按钮即可。

步骤6 用户也可以在【指定的文件类型】列表框中选择某个文件扩展名，然后单击 删除(R) 按钮，打开【软件限制策略】对话框，单击 是(Y) 按钮删除该种文件类型。




(2) 通过【系统】选项设置

步骤1 打开【本地组策略编辑器】窗口，依次展开【本地计算机 策略】➤【用户配置】➤【管理模块】➤【系统】选项，然后在右侧的窗格中找到并双击【只运行指定的Windows应用程序】菜单项。

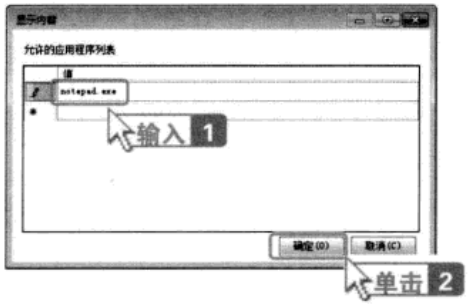
步骤2 打开【只运行许可的Windows应用程序】窗口，选中【已启用】单选钮，此时【允许的应

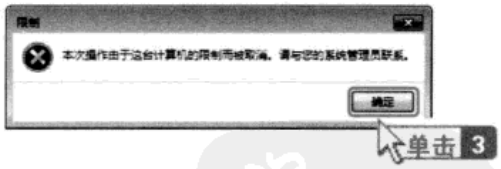
用程序列表】右侧的显示... 按钮被激活，单击该按钮。



步骤3 打开【显示内容】窗口，在默认情况下，【允许的应用程序列表】列表框中是空白无内容的，用户可以在文本框中输入想要设置为允许运行的应用程序的名称，这里输入“notepad.exe”，然后单击 确定(O) 按钮即可完成允许运行的应用程序设置，没有显示在【允许的应用程序列表】列表框中的应用程序是不能运行的。

步骤4 当用户运行某个未被添加到【允许的应用程序列表】中的程序时，会弹出【限制】对话框，提示用户操作已被取消。




## 7.2.4 设置本地计算机安全策略

安全是计算机用户所不能忽视的一个方面。设置完善的安全策略对于维护计算机系统的安全是很重要的。下面介绍系统安全管理和IP安全策略管理的方法。

### 1. 系统安全管理

系统的安全是至关重要的，它不仅影响着计算机能否处于一个稳定且安全可靠的环境中，而且直接影响着用户的权益能否得到有效的保障。一些网络攻击者常常利用用户计算机中的漏洞进行窃取和破坏活动，从而给用户带来不必要的损失。在与本地安全策略相关的策略选项

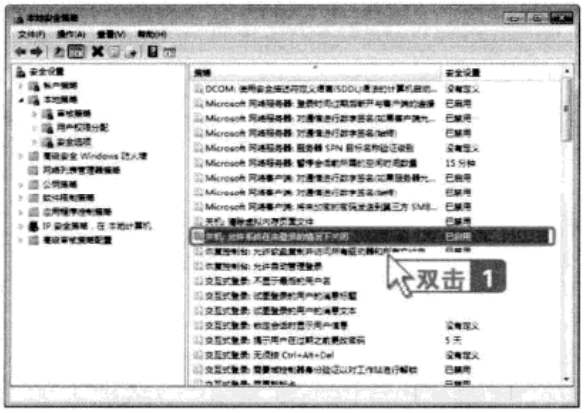
中，有一些是与系统安全紧密相关的，对这些策略选项进行适当的设置，能够更好地维护计算机系统的安全。

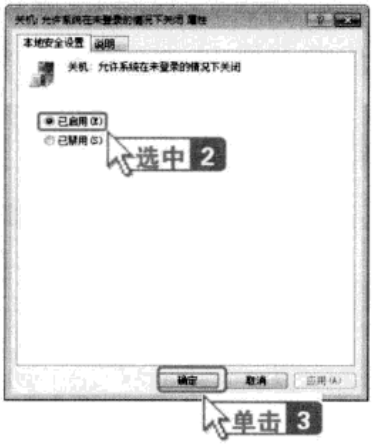
## 禁止登录前关机

禁止在登录前关机，用户只有成功登录到计算机并具有关闭系统用户权限后，才能够通过桌面执行系统关闭操作。设置禁止在登录前关机的具体步骤如下。

步骤1 选择【开始】➢【运行】菜单项，打开【运行】对话框，在【打开】文本框中输入“secpol.msc”命令，按下【Enter】键打开【本地安全策略】窗口，并在左侧窗格中依次展开【安全设置】➢【本地策略】➢【安全选项】选项，接着在右侧窗格中找到并双击【关机：允许系统在未登录的情况下关闭】选项。

步骤2 打开【关机：允许系统在未登录的情况下关闭 属性】对话框，默认情况下，该策略选项的设置值为【已启用】。如果用户的计算机是作为服务器使用的，则可选中【已禁用】单选钮；如果作为终端机使用，则可选中【已启用】单选钮，然后单击 确定 按钮即可。




### 为什么作为服务器和终端机时的设置不同？

通常情况下，作为服务器的计算机由于其是作为众多终端机的一个服务端，许多资源都需要从该服务器上下载，因此它是否能够保证运行正常、不受到恶意攻击和不中途断电关机等，对于局域网甚至是整个Internet都起着至关重要的作用，因此应该将该策略选项设置为【已禁用】。而对于作为终端机的计算机来说，不需要保证计算机一直都处于开机状态，如果用户在进入登录界面以后不想使用计算机了，则在登录界面上有一个【关闭计算机】选项便会显得很方便。

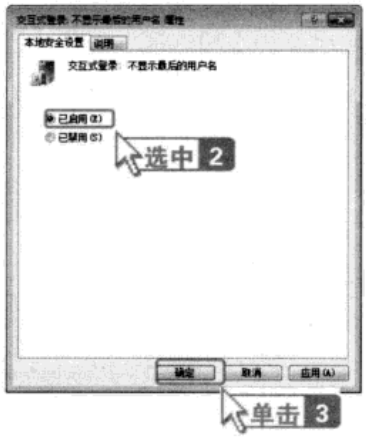
## 不显示最后登录的用户名

在登录计算机系统时，最后一次登录的用户名会显示在Windows登录界面上。这有可能造

成用户名的泄露，给一些别有用心的人可乘之机。用户可以通过设置【安全选项】来让最后一次成功登录的用户名不显示在Windows登录界面中。具体的操作步骤如下。

步骤1 打开【本地安全策略】窗口，然后在左侧窗格中依次展开【安全设置】➤【本地策略】➤【安全选项】选项，在右侧窗格中找到并双击【交互式登录：不显示最后的用户名】选项。

步骤2 打开【交互式登录：不显示最后的用户名 属性】对话框，选中【已启用】单选钮，然后单击 确定 按钮即可。

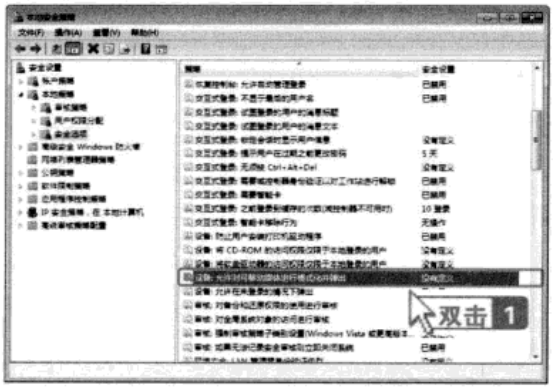



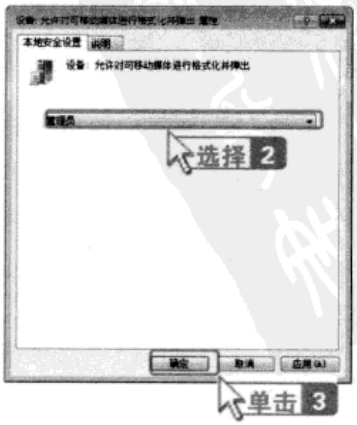

## 限制格式化和弹出可移动媒体

通过限制格式化和弹出可移动媒体可以防止未经授权的用户从一台计算机中读取媒体，然后从他们具有本地管理员特权的另一台计算机中访问该媒体。具体的操作步骤如下。

步骤1 打开【本地安全策略】窗口，然后在左侧窗格中依次展开【安全设置】➤【本地策略】➤【安全选项】选项，在右侧窗格中找到并双击【设备：允许对限制格式化和弹出可移动媒体】选项。

步骤2 打开【设备：允许对限制格式化和弹出可移动媒体 属性】对话框，在下拉列表中一共包括3个设置选项，用户可以根据实际情况进行设置，这里选择【管理员】选项，然后单击 确定 按钮即可。



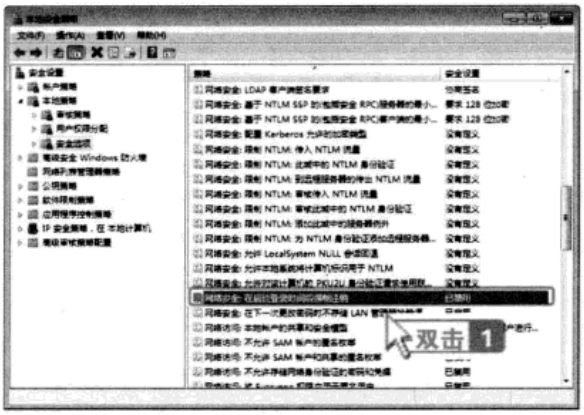



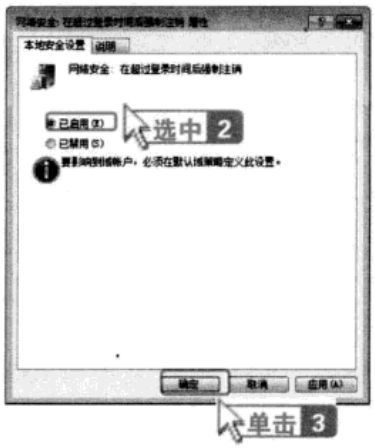
## 在超时登录时强制注销

该策略选项用来确定当用户连接到本地计算机上且已超过用户账户的有效登录时间时，是否断开该用户。该设置影响【服务器消息块（SMB）】组件。设置该策略选项的具体步骤如下。

步骤1 打开【本地安全策略】窗口，然后在左侧窗格中依次展开【安全设置】➤【本地策略】➤【安全选项】选项，在右侧窗格中找到并双击【网络安全：在超过登录时间后强制注销】选项。

步骤2 打开【网络安全：在超过登录时间后强制注销 属性】对话框，默认情况下，该策略选项选中的是【已禁用】单选钮，选中【已启用】单选钮，然后单击 确定 按钮即可。




### 为什么该策略选项可以作为账户策略？

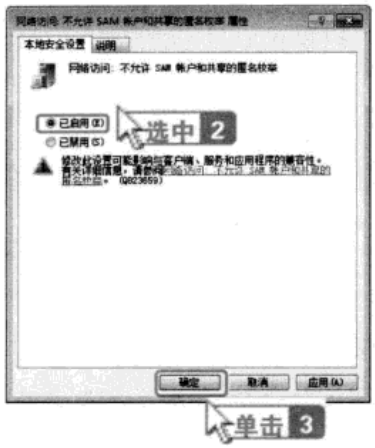
该策略选项可以作为账户策略。对于域账户，只有一种账户策略。账户策略必须在默认域策略中定义，并且由组成该域的域控制器实施。域控制器始终从【默认域策略组策略对象（GPO）】中提取账户策略，即使存在应用到该域控制器所在的组织单位的不同账户策略。默认情况下，加入到域中的工作站和服务器也同样会接收到各自本地账户的相同账户策略。然而，通过为该成员计算机所在的组织单位定义账户策略，可以使成员计算机的本地账户策略不同于域账户策略。

## 不允许 SAM 账户和共享的匿名枚举

Windows允许匿名用户执行某些活动，如枚举域账户和网络共享名。当管理员要给一个不需要维护相互信任关系的信任域中的用户进行访问授权时，这是非常方便的。如果用户不想允许匿名枚举SAM账户和共享，则可启用该策略。设置不允许SAM账户和共享的匿名枚举的具体步骤如下。

步骤1 打开【本地安全策略】窗口，然后在左侧窗格中依次展开【安全设置】➤【本地策略】➤【安全选项】选项，在右侧窗格中找到并双击【网络访问：不允许SAM账户和共享的匿名枚举】选项。

步骤2 打开【网络访问：不允许SAM账户和共享的匿名枚举 属性】对话框，默认情况下，该策略选项选中的是【已禁用】单选钮，选中【已启用】单选钮，然后单击 确定 按钮即可。


### 不允许 SAM 账户和共享的匿名枚举能够预防攻击？

SAM账户和共享的匿名枚举能够方便用户执行某些操作，但是，这也可能成为一些网络攻击者利用字典破解的攻击对象，将该策略选项设置为【已启用】，能够有效地预防这种攻击。如果用户想要允许的话，也可以设置为【已禁用】。

## 设置本地账户的共享和安全模型

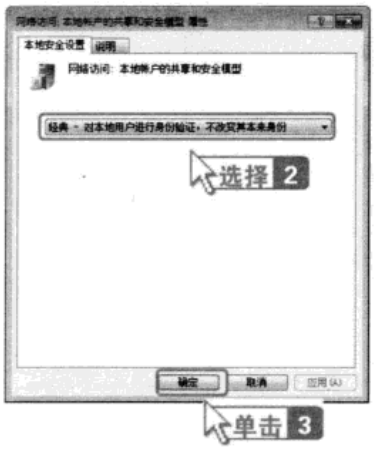
在使用网络共享多台计算机时，为了保证用户信息的安全，可以对本地账户的网络登录进行身份验证。设置本地账户的共享和安全模型的具体步骤如下。

步骤1 打开【本地安全策略】窗口，然后在左侧窗格中依次展开【安全设置】➢【本地策略】➢【安全选项】选项，在右侧窗格中找到并双击【网络访问：本地账户的共享和安全模型】选项。

步骤2 打开【网络访问：本地账户的共享和安全模型 属性】对话框，在下方的下拉列表中共包括两个设置选项，即【经典–对本地用户进行身份验证，不改变其本来身份】和【仅来宾–对本地用户进行身份验证，其身份为来宾】选项，用户可以选择一个想要设置的选项，然后单击 确定 按钮即可。

### 该策略选项属性中的两个设置选项各自的作用是什么？

如果使用【仅来宾–本地用户以来宾身份验证】选项，则使用本地账户的网络登录会自动映射到来宾账户，并且任何可以通过网络访问用户计算机的用户（包括匿名的Internet用户）都可以访问用户的共享资源。如果使用【经典–本地用户以自己的身份验证】选项，则使用本地账户凭据的网络登录会使用这些凭据进行身份验证。另外，应该使用密码来保护本地账号，否则任何人都可以使用这些账户来访问共享资源。


## 2. IP 安全策略管理

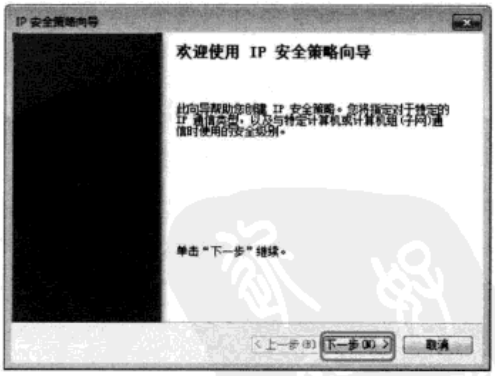
IP安全策略的设置很重要。没有安全设置，公用网和专用网就容易遭受未经授权的监视和访问。内部攻击可能源于Intranet内薄弱的安全保护。来自专用网络之外的危险则源于与Internet和Intranet的连接，仅有基于密码的用户访问控制并不能保护通过网络传输的数据。

用户可以创建并定义适合自己的IP安全策略，从而给计算机系统提供一个更加安全的环境。在Windows的本地安全策略设置中，用户可以创建并定义相应的IP安全策略。

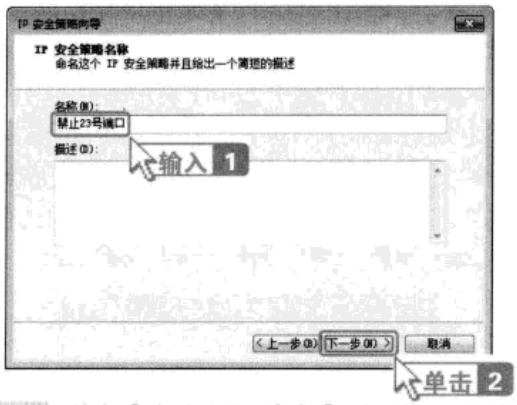
下面以禁止23号端口为例来介绍创建并定义IP安全策略的具体步骤。

步骤1 选择【开始】➤【运行】菜单项，打开【运行】对话框，在【打开】文本框中输入“secpol.msc”命令并按下【Enter】键，打开【本地安全设策略】窗口，在左侧窗格中选择【IP安全策略，在本地计算机】选项，并单击鼠标右键，从弹出的快捷菜单中选择【创建IP安全策略】菜单项。

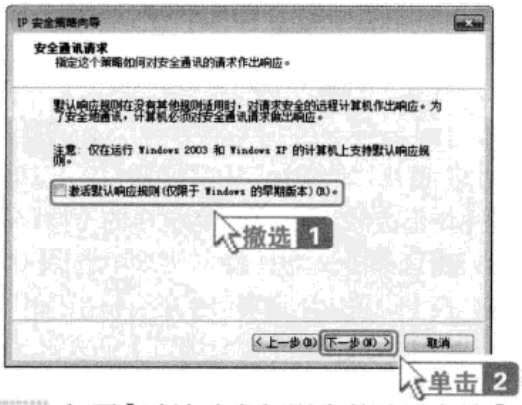
步骤2 打开【IP安全策略向导】对话框，然后单击下一步(N) >按钮。



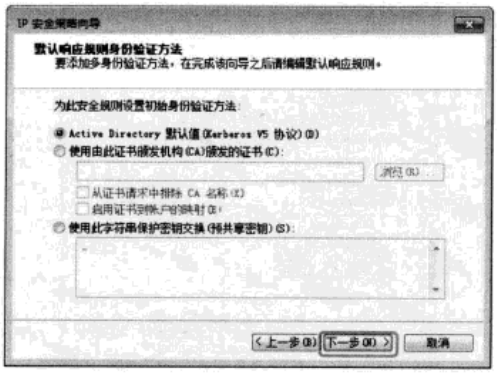

步骤3 打开【IP安全策略名称】对话框，在这里用户可以设置所创建的IP安全策略的名称以及描述，这里将名称命名为“禁止23号端口”，描述为空，然后单击下一步(N) >按钮。



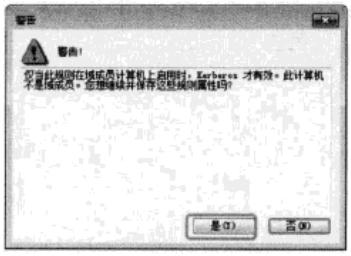

步骤4 弹出【安全通讯请求】对话框，取消选中【激活默认响应规则（仅限于Windows的早期版本）】复选框，并单击下一步(N) >按钮。



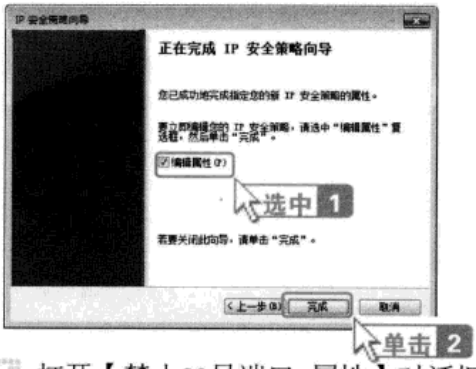

步骤5 打开【默认响应规则身份验证方法】对话框，这里采用默认设置，然后单击下一步(N) >按钮。



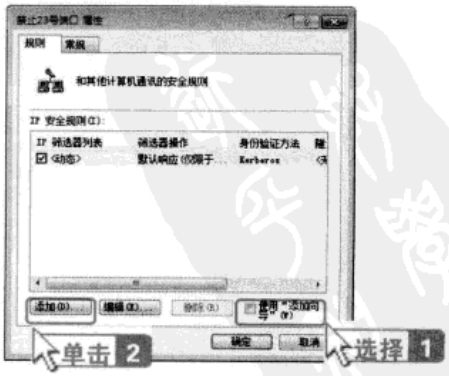

步骤6 弹出【警告】对话框，提示用户仅当此规则在域成员计算机启用时，Kerberos才有效，单击是(Y)按钮。




步骤7 打开【正在完成IP安全策略向导】对话框，选中【编辑属性】复选框，然后单击完成按钮。



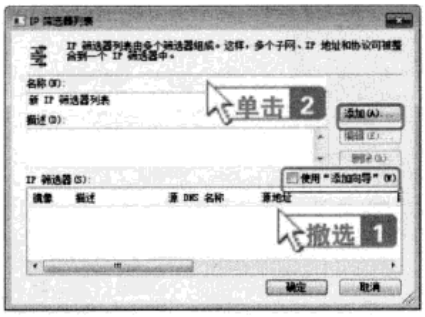

步骤8 打开【禁止23号端口 属性】对话框，选中【使用“添加向导”】复选框，然后单击添加(D)...按钮。




步骤9 弹出【新规则 属性】对话框，并单击

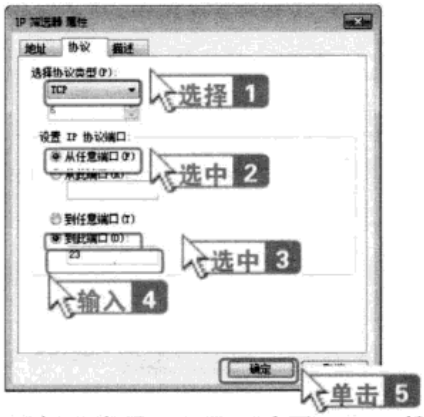
添加(D)...按钮。

步骤10 打开【IP筛选器列表】对话框，取消选中【使用“添加向导”】复选框，单击添加(A)...按钮。

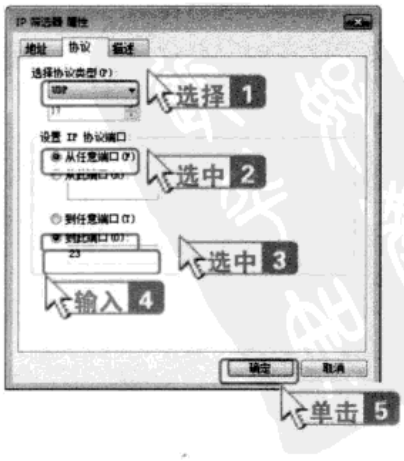



步骤11 打开【IP筛选器 属性】对话框，在【源地址】和【目标地址】下拉列表中分别选择【任何IP地址】和【我的IP地址】选项。


步骤12 切换到【协议】选项卡，在【选择协议类型】下拉列表中选择【TCP】选项，在【设置IP协议端口】组合框中选中【从任意端口】单选钮和【到此端口】单选钮，然后在【到此端口】下面的文本框中输入“23”。最后单击确定按钮即可添加一个屏蔽TCP协议23号端口的筛选器。




步骤13 重复“步骤10”和“步骤11”，然后切换到【IP筛选器 属性】对话框中的【协议】选项卡，在【选择协议类型】下拉列表中选择【UDP】选项，在【设置IP协议端口】组合框中选中【从任意端口】单选钮和【到此端口】单选钮，然后在【到此端口】下面的文本框中输入“23”。最后单击确定按钮即可添加一个屏蔽UDP协议23号端口的筛选器。



步骤14 返回【IP筛选列表】对话框，单击 确定 按钮，返回【新规则 属性】对话框，在这里所选的IP筛选器列表指定了其网络流量受此规则影响，接着在【IP筛选器列表】列表框中选中【新IP筛选器列表】单选钮。

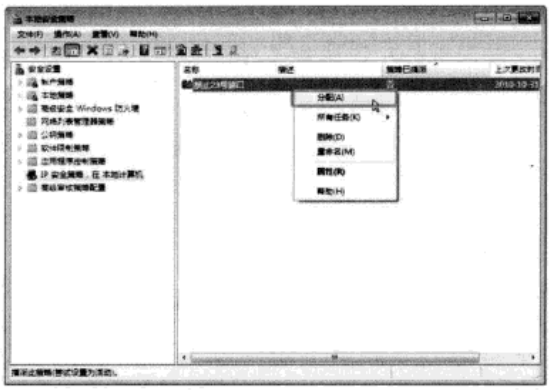
步骤15 切换到【筛选器操作】选项卡，取消选中【使用“添加向导”】复选框，单击 添加(D)... 按钮。


步骤16 打开【新筛选器操作 属性】对话框，切换到【安全方法】选项卡，选中【阻止】单选钮，然后单击 确定 按钮。


步骤17 返回【新规则 属性】对话框，可以发现在【筛选器操作】列表框中增加了一个【新筛选器操作】选项，在这里选择的筛选器操作指定了此规则是否协商以及如何保证网络流量的安全。接着选中【新筛选器操作】单选钮，然后单击 关闭 按钮。


步骤18 返回【禁止23号端口 属性】对话框，用户可以发现在【IP安全规则】列表框中增加了一个【新IP筛选器列表】选项，并且其左边的复选框呈选中状态，单击 确定 按钮，即可添加一个禁止23号端口的IP安全策略。

步骤19 重新进入【本地安全设置】窗口中，并在右侧窗格中的【禁止23号端口】选项上单击鼠标右键，从弹出的快捷菜单中选择【分配】菜单项，最后重新启动计算机即可使设置生效。



## 7.3 使用防木马软件和杀毒软件

无可非议，杀毒软件在维护系统安全及查杀病毒方面的功能不可忽视。使用杀毒软件，用户可以很快地发现潜藏在计算机中的病毒和木马，然后将其清理。

### 7.3.1 使用防木马软件

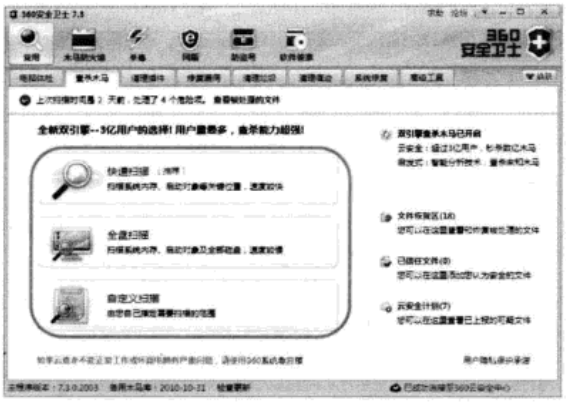
#### 1. 360 安全卫士

360安全卫士拥有查杀木马、清理插件、修复漏洞、电脑体检等多种功能，并独创了“木马防火墙”功能，依靠抢先侦测和云端鉴别，可全面、智能地拦截各类木马，保护用户的账号、隐私等重要信息。目前木马威胁之大已远超病毒，360安全卫士运用云安全技术，能有效防止个人数据和隐私被木马窃取。360安全卫士占用的存储空间小，同时还具备开机加速、垃圾清理等多种系统优化功能，内含的360软件管家还可以帮助用户轻松下载、升级和强力卸载各种应用软件。

使用360安全卫士查杀流行木马的具体步骤如下。

步骤1 在计算机上安装360安全卫士之后，运行该程序，打开程序主窗口，切换到【查杀木马】选项卡，在此用户可以根据需要选择扫描方式，包括【快速扫描（推荐）】、【全盘扫描】和【自定义扫描】3种。

步骤2 单击相应的扫描方式图标，即可进行木马扫描，如果在计算机中发现木马程序，用户可以将其选中，然后单击 立即处理 按钮将其清理。



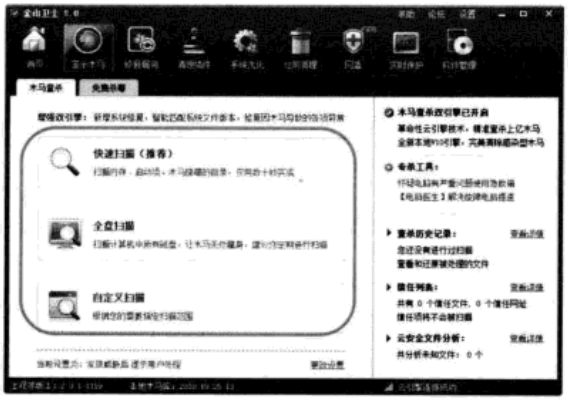


### 2. 金山卫士

金山卫士是查杀木马的能力更强、检测漏洞更快、体积更小巧的免费安全软件。它采用双引擎技术，云引擎能查杀上亿已知木马。漏洞检测针对Windows 7优化，更有实时保护、软件管理、插件清理、修复IE、启动项管理等功能，能够全面保护用户的系统安全。金山卫士与360安全卫士查杀木马的方法非常相似，具体的操作步骤如下。

步骤1 安装并运行“金山卫士”程序，打开其主窗口，并切换到【查杀木马】选项卡，在此用户可以根据需要选择扫描方式，包括【快速扫描】、【全盘扫描】和【自定义扫描】3种。

步骤2 单击相应的扫描方式图标，即可进行木马扫描，如果在计算机中发现木马程序，用户可以将其选中，然后单击 立即处理 按钮将其清理。





## 7.3.2 使用杀毒软件

### 1. 360 杀毒软件

360杀毒软件整合了国际知名的BitDefender病毒查杀引擎，以及360安全中心领先的云查杀

引擎，双引擎智能调度，能够为用户提供完善的病毒防护体系。下面介绍如何利用360杀毒软件进行病毒的查杀。

步骤1 安装并运行“360杀毒软件”程序，打开其主窗口，并切换到【病毒查杀】选项卡，在此通过单击【快速扫描】按钮、【全盘扫描】按钮和【指定位置扫描】按钮选择需要扫描的方式。

步骤2 这里单击【快速扫描】按钮，即可进行木马扫描。



步骤3 扫描完成后，单击 开始处理 按钮进行病毒的清理即可。


## 2. 卡巴斯基杀毒软件

卡巴斯基反病毒软件具有一套全新的安全解决方案，它可以保护用户计算机免受病毒、蠕虫、木马和其他恶意程序的危害，并能够实时监控文件、网页、邮件、QQ/MSN协议中的恶意对象，阻止指向恶意网站的链接，其强大的主动防御功能和病毒查杀功能为用户的系统安全提供了有利保障。

下面介绍如何使用“卡巴斯基反病毒软件 2011”来查杀木马、病毒以及恶意程序等。

步骤1 安装并运行“卡巴斯基反病毒软件 2011”程序，接着打开其主窗口，然后单击 按钮。

步骤2 切换到【智能查杀】选项卡，在此通过单击【开始全盘扫描】按钮和【开始关键区扫描】按钮选择需要扫描的方式。另外，用户还可以进行自定义扫描，单击下方的按钮或者【浏览】链接，进行文件的自定义选择。



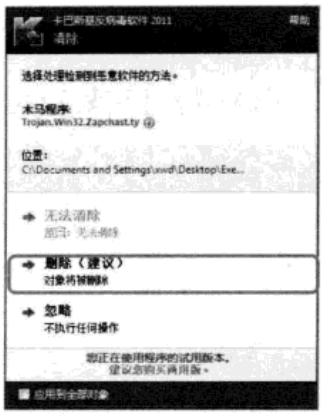
步骤3 弹出【自定义扫描】对话框，在其列表框中，用户可以通过选中复选框来选择想要扫描的位置，这里选中【本地磁盘（C:）】和【本地磁盘（D:）】复选框。

步骤4 用户还可以在【自定义扫描】对话框的文本框中添加、编辑或删除其他对象，这里单击 添加 按钮，弹出【选择扫描对象】对话框，在其列表框中选择要添加的对象，例如选择桌面，接着在下方的【对象】文本框中可以看到该对象的路径，然后选中【包含子文件夹】复选框并单击 确定 按钮。



步骤5 返回【自定义扫描】对话框，可以看到该对象添加到其列表框中了，然后单击 确定 按钮即可自动进行扫描。

步骤6 由于是第一次安装该杀毒软件，最好先进行一次全盘扫面，单击【开始全盘扫描】按钮进行扫描，扫描过程中，如果扫描到木马、病毒或恶意程序等，卡巴斯基软件会弹出对话框，例如下方弹出的对话框中提示用户检测到木马程序，用户可以单击【删除（建议）】按钮将其删除。


## 7.4 使用网络防火墙

随着网络的逐渐普及，网络攻击也成为了一种常见的现象。网络攻击不同于病毒，它有可能给用户带来无法想象的损失。因此，抵御网络攻击便显得尤为重要。安装并使用防火墙能够有效地抵御网络攻击，给用户的系统安全带来保障。

### 7.4.1 使用系统自带的防火墙

防火墙是指由软件或软、硬件组合而成，位于内部网络和外部网络、专用网与公共网之间的保护屏障，根据访问安全策略对流入、流出的通信数据进行扫描，过滤掉不允许的流入数据或禁止特定端口的流出数据，对电脑起着重要的保护作用。

在Windows 7操作系统中，微软公司进一步调整了防火墙的功能，更改了高级设置的访问方式，把Windows Vista中隐藏的功能公开化了，并且增加了更多的网络选项，支持多种防火墙策略，让防火墙更加便于用户使用，特别适用于移动型计算机。

Windows 7的防火墙位于【控制面板】➢【系统和安全】功能区，打开【Windows防火墙】的初始界面。


在Windows 7中共有4种网络类型，分别是【公用网络】、【家庭网络】、【工作网络】和【域】，其中【家庭网络】和【工作网络】都被视为私人网络，操作系统会根据所选择的网络类型自动设置适当的防火墙和安全设置，这样用户在不同的位置连接网络时，只要选择合适的网络位置，就可以确保始终将电脑设置为适当的安全级别。

在Windows 7操作系统中，防火墙可以通过【Windows防火墙】窗口进行设置，其中包括基本设置和高级设置两种方法。

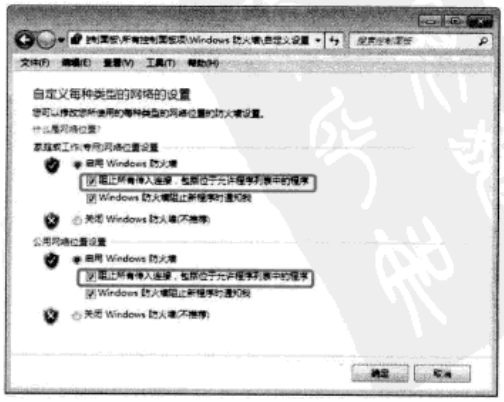
## 1. 防火墙的基本设置

基本设置方法适用于普通电脑用户，可通过简单的设置，打开或关闭防火墙，更改通知设置，允许程序或功能通过Windows防火墙。如果设置混乱，还可以还原为默认设置，从而实现对系统的有效保护。下面介绍Windows 7防火墙的基本设置方法。

步骤1 打开【Windows防火墙】窗口，可以看到左侧窗格中有【允许程序或功能通过Windows防火墙】、【更改通知设置】、【打开或关闭Windows防火墙】、【还原默认设置】和【高级设置】等链接，在主窗口中显示了当前的网络类型和状态，用户可以通过单击除了【高级设置】以外的链接来对防火墙进行简单的设置。

步骤2 单击【更改通知设置】和【打开或关闭Windows防火墙】链接，都会弹出【自定义设置】窗口，可以看到【家庭或工作（专用）网络位置设置】和【公用网络位置设置】下都有【启用Windows防火墙】和【关闭Windows防火墙】两个单选钮，【启用Window防火墙】选项下还有两个复选框，默认选中【Windows防火墙阻止新程序时通知我】复选框，这样防火墙发现可信任列表以外的程序访问用户计算机时，会弹出阻止对话框进行提示，如果这个程序是用户正在使用的或允许的，用户就可以通过进一步的设置将这个程序添加到防火墙中的可信任程序列表中。

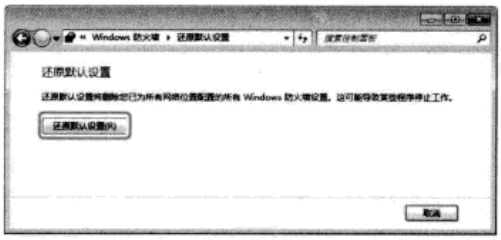
步骤3 在连接到机场或旅馆的公用网络时，如果希望防火墙阻止所有的程序，可以选中【阻止所有传入连接，包括位于允许程序列表中的程序】复选框，此时Windows防火墙会阻止包括可信任程序在内的大多数程序。需要注意的是：把防火墙设置为这种状态，仍然可以浏览大多数的网页、收发电子邮件和查阅即时消息。



步骤4 如果用户已经安装了第三方的防火墙程序，或想暂时禁用Windows自带的防火墙，可以选中【关闭Windows防火墙（不推荐）】单选钮，然后单击 确定 按钮，这样就关闭了Windows自带的防火墙。

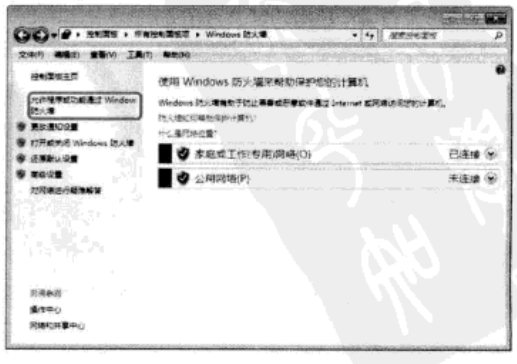
步骤5 在【自定义设置】窗口中，Windows 7 的防火墙还可以分别对【家庭或工作网络】、【公用网络】选项进行设置，这样当用户的电脑同时连接到不同的网络时，可以针对每种网络分别使用不同的防火墙规则。例如，这里在【家庭或工作网络】选项中，防火墙采用了默认设置；在【公用网络】选项中，防火墙阻止了所有的连接。单击 确定 按钮返回【Windows防火墙】窗口，用户可以看到这两个选项的设置状态。

步骤6 如果是因为防火墙的错误设置，导致用户网络出现了故障，还可以通过单击【Windows防火墙】窗口中的【还原默认设置】链接，将其还原到默认设置。当单击【还原默认设置】链接后，会弹出【还原默认设置】窗口，单击 还原默认设置(R) 按钮，即可将Windows防火墙还原到默认设置状态。



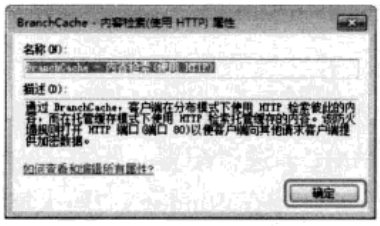
Windows 7中的防火墙可以自动把用户允许的程序添加到可信任程序列表中，因此一般不需要手动添加程序。实际上管理防火墙可信任列表中的程序更简单，操作更方便。

步骤1 打开【Windows防火墙】窗口，单击左侧窗格中的【允许程序或功能通过Windows防火墙】链接。



步骤2 打开【允许的程序】窗口，在窗口中显示了一些程序的列表（但为不可用状态），如果用户想查看程序的详细信息，则单击 更改设置(N) 按钮，列表框中显示可用状态，然后选择需要了解的程序，单击 详细信息(L)... 按钮。

步骤3 弹出该程序的详细属性，查看完成后，单击 确定 按钮即可。

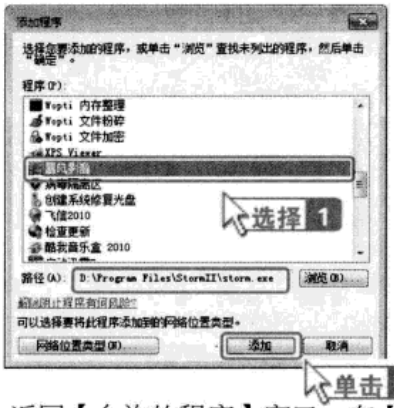


步骤4 如果选择了Windows自带组件以外的程序，则会列出详细的路径和文件名称，帮助用户判断是否有必要允许、阻止或删除该程序，此时 删除(M) 按钮也为可用状态。

步骤5 如果用户想把Windows自带组件以外的程序从列表中删除，可以先选择需要删除的程序，然后单击 删除(M) 按钮，弹出【删除程序】对话框，提示删除该程序可能引起的问题。如果想暂时禁用，可以在列表中取消选中该程序的复选框。如果用户确认要删除该程序，则可单击 是(Y) 按钮，否则单击 否(N) 按钮。

步骤6 列表框中列出的每个程序都有【家庭/工作（专用）】和【公用】两种网络类型可以供选择，用户可以选择或取消选中程序前面的复选框来允许或阻止它通过防火墙，也可以选择这两种网络类型的一种或全部。

步骤7 如果用户想要手动添加允许的程序，操作也很简单，在【允许的程序】窗口中单击 允许运行另一程序(R)... 按钮，弹出【添加程序】对话框。列表中显示了操作系统找到的程序，选择一个程序后会在【路径】文本框中显示该程序的路径信息，然后单击 添加 按钮。





步骤8 返回【允许的程序】窗口，在【允许的程序和功能】列表框中可以看到添加进来的程序，然后用户便可以对其进行其他设置。

## 为什么可以放心地删除允许的程序?

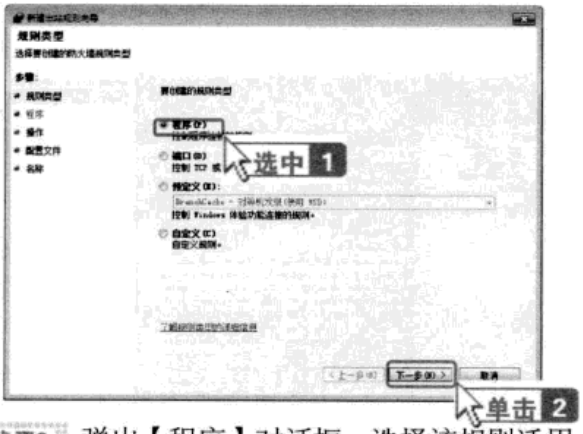
因为Windows的内置组件只能被允许或阻止，而无法删除，所以用户可以放心地删除允许的程序，在正常的程序需要通过防火墙，出现【Windows防火墙已经阻止此程序的部分功能】对话框时，选择允许通过或再把程序添加到列表中即可。

### 2. 防火墙的高级设置

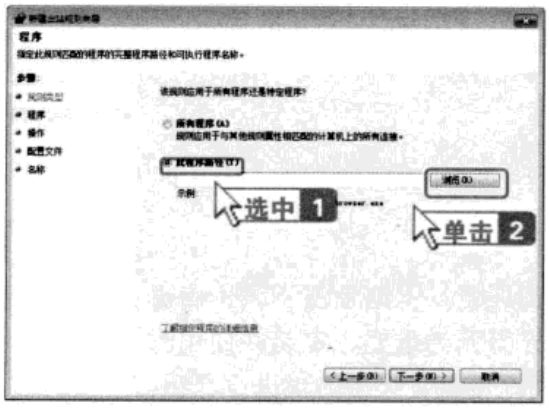
如果用户感觉Windows防火墙的基本设置不能满足要求，还可以进行Windows防火墙的高级设置。Windows 7的防火墙可以通过微软管理控制台（MMC）进行配置，既可以创建入站规则，又可以创建出站规则。下面以阻止QQ游戏的运行为例，介绍在Windows 7防火墙中如何创建出站规则。

步骤1 打开【Windows防火墙】窗口，单击【高级设置】链接，打开【高级安全Windows防火墙】窗口，在左侧窗格中选择【出站规则】选项，然后单击右侧窗格中的【新建规则】选项。

步骤2 弹出【规则类型】对话框，显示了可以用来创建规则的4种类型，其中【程序】是通过指定程序的可执行（.exe）文件来允许程序通过防火墙，默认下情况允许程序接受任何端口上的连接。【端口】是通过指定协议（TCP或UDP）和本地端口，允许使用这些端口的程序通过防火墙。【预定义】列表显示系统中主要的服务和程序，用户可以从中选择进行设置。【自定义】提供了最大限度的设置选项，用户可以创建未包含在以上类型的其他规则。在这里选中【程序】单选钮，然后单击 下一步(N) > 按钮。

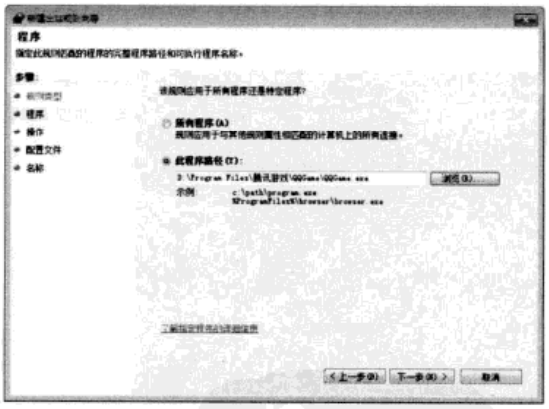



步骤3 弹出【程序】对话框，选择该规则适用的程序，可以选择所有的程序或指定某个程序。在此选中【此程序路径】单选钮，然后单击 浏览(R)... 按钮。

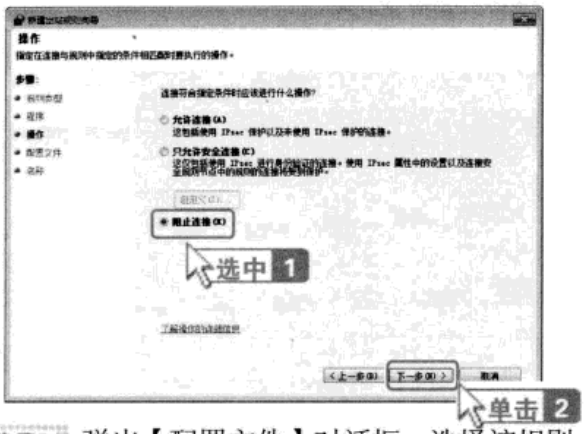



步骤4 弹出【打开】对话框，选中QQ游戏的可执行文件“QQGame.exe”，单击 打开(O) 按钮。

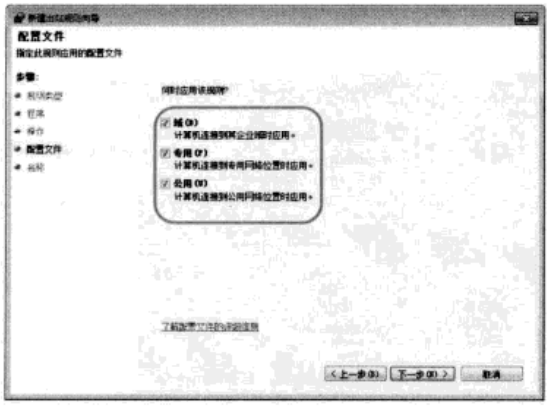
步骤5 返回【程序】对话框，在【此程序路径】文本框中显示了程序的路径和名称，然后单击 下一步(N) > 按钮。



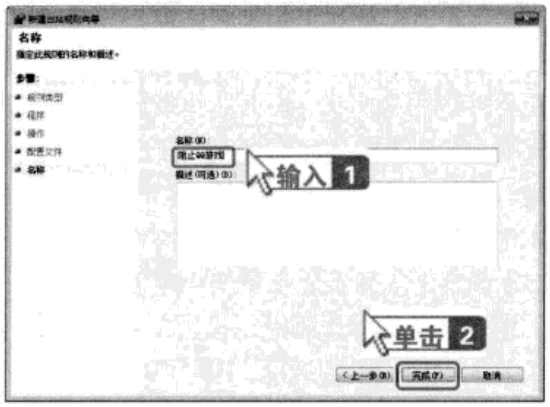
步骤6 弹出【操作】对话框，有3个单选钮，其中【允许连接】允许符合规则设定的网络数据包通过防火墙。【只允许安全连接】仅允许受IPsec（Internet Protocol Security，互联网协议安全）保护的连接，IPsec设置需要在单独的连接安全规则中定义。【阻止连接】则阻止所有的网络数据包。在此保持系统的默认选项【阻止连接】不变，单击 下一步(N) > 按钮。



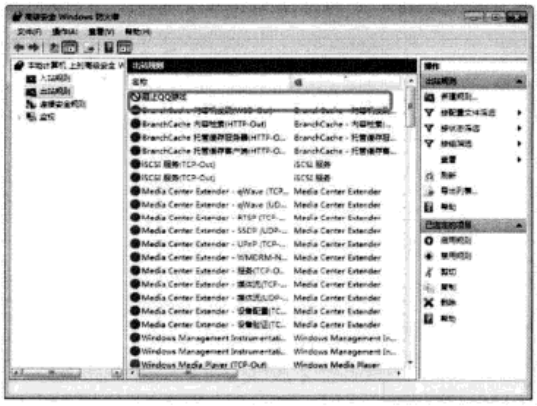

步骤7 弹出【配置文件】对话框，选择该规则在何时应用，有【域】、【专用】和【公用】等3个复选框，默认3个复选框全部选中，用户可以根据计算机的位置选择。在这里保持默认设置，然后单击 下一步(N) > 按钮。



步骤8 弹出【名称】对话框，在【名称】文本框中输入该规则的名称“阻止QQ游戏”，还可以在【描述】文本框中输入该规则的描述信息，然后单击 完成(F) 按钮。




步骤9 稍后就可以在【高级安全Windows防火墙】窗口中看到新建的出站规则“阻止QQ游戏”，此时用户运行QQ游戏，就会被防火墙阻止。



用户可以更改规则的选项设置，在需要更改的规则上双击鼠标，在弹出的对话框进行设置即可。

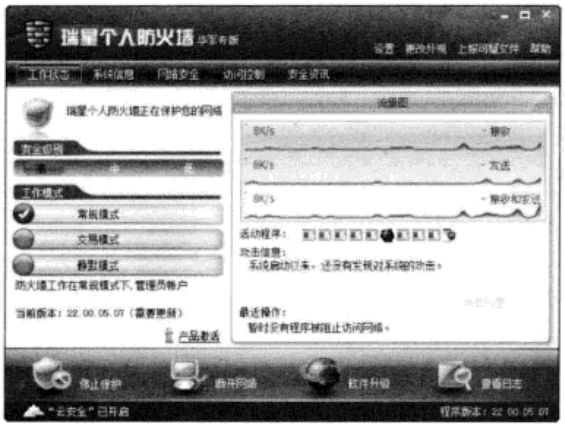
## 7.4.2 使用第三方网络防火墙

随着网络的普及，网络攻击也成为了一种常见的现象。网络攻击不同于病毒，它可能会给用户带来无法想象的损失。因此，抵御网络攻击便显得尤为重要。安装并使用防火墙能够有效地抵御网络攻击，给用户的系统安全带来保障。下面以瑞星防火墙为例进行介绍。

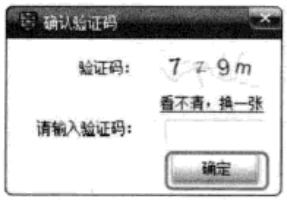
## 1. 瑞星个人防火墙主界面

瑞星防火墙是一款功能非常强大的国产软件，它具有完备的规则设置，能有效地监控任何一个网络连接。瑞星个人防火墙2010融入了“云安全”计划，防御能力大大增强。

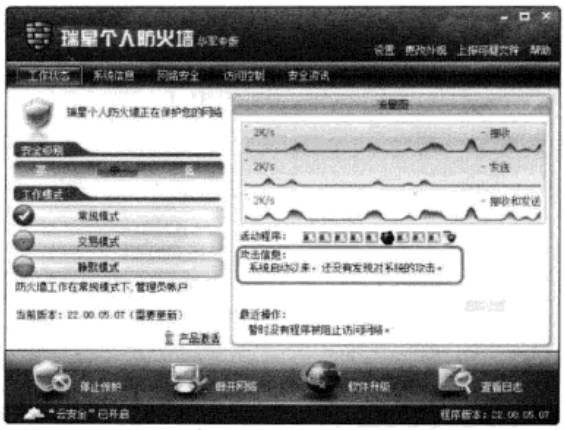
步骤1 安装并运行【瑞星个人防火墙】程序，打开【瑞星个人防火墙】窗口。




步骤2 单击窗口工具栏中的按钮，即可进行相应的操作。在左侧窗格的【安全级别】组合框中选择想要设置的安全级别，这里单击 中 按钮，会弹出【确认验证码】对话框，在【请输入验证码】对话框中输入验证码，输入完毕单击 确定 按钮即可完成设置。

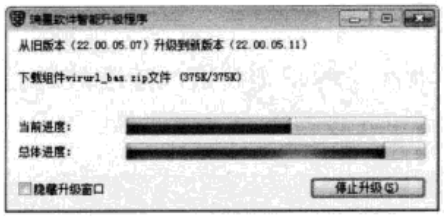



步骤3 在【工作模式】组合框中列出了3种不同的工作模式，用户可以根据自己的需要选择。右侧窗格中显示了接收和发送的数据流量，以及当前正在访问网络的程序。在【攻击信息】组合框中可以看到用户电脑受攻击的信息。

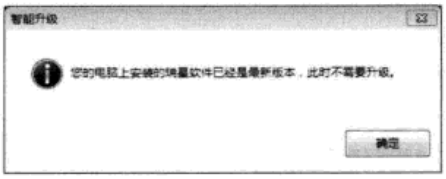



步骤4 单击窗口下方组合框中的【停止保护】按钮，即可将瑞星个人防火墙关闭，此时【停止保护】按钮变成【开启保护】按钮。

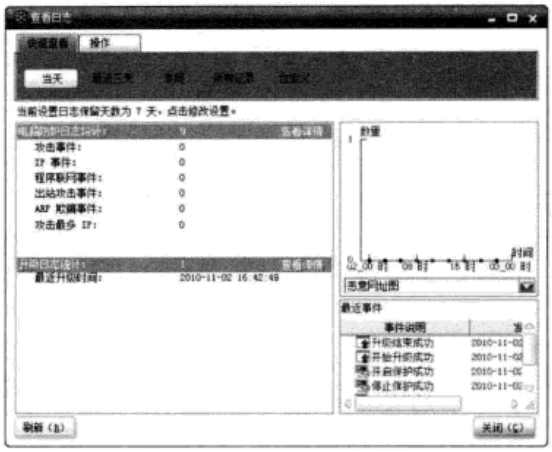

步骤5 单击【软件升级】按钮，弹出【智能升级正在进行...】对话框，瑞星防火墙将检测最新版本，开始自动升级软件。




步骤6 若瑞星防火墙为最新版本，则会提示用户不需要升级。




步骤7 单击【查看日志】按钮，弹出【查看日志】窗口，其中显示了电脑的【防护日志统计】和【升级日志统计】的详细信息。




## 2. 瑞星防火墙规则设置

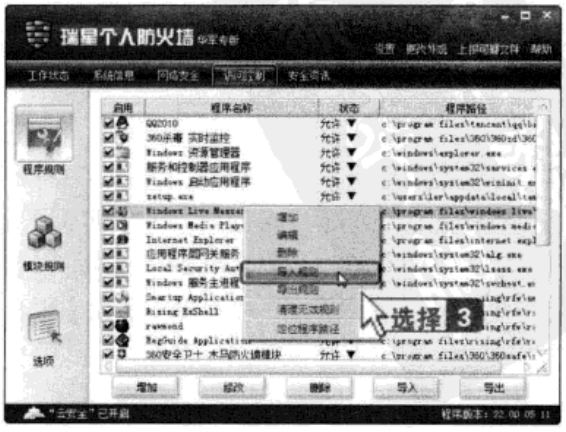
瑞星防火墙规则设置用于配置防火墙的过滤规则，提高其拦截能力，以便更好地保护用户电脑的安全。

### 增加规则

增加规则分为增加程序规则和增加模块规则两个方面，增加规则的具体步骤如下。

步骤1 单击窗口工具栏中的【访问控制】按钮 访问控制，进入【访问控制】界面，单击左侧窗格中的【程序规则】按钮，在右侧窗格中显示系统中受控制的程序。

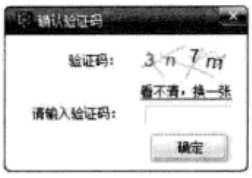
步骤2 在想要增加规则的程序上单击鼠标右键，从弹出的快捷菜单中选择【导入规则】菜单项。


步骤3 弹出【确认验证码】对话框，在【请输入验证码】对话框中输入验证码，输入完毕单击 确定

按钮。

步骤4 弹出【请选择要导入的规则文件】对话框，从中选择要导入的规则文件，选择完毕单击 打开(O) 按钮即可。按照相同的方法还可以进行【模块规则】的添加。



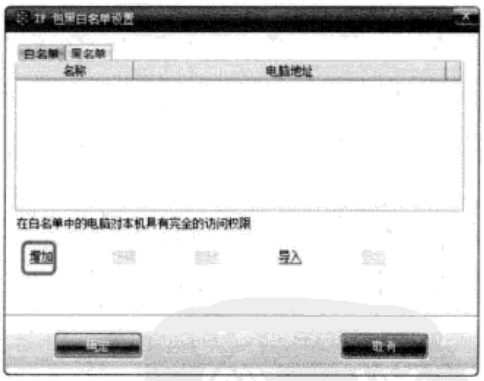


## 设置规则

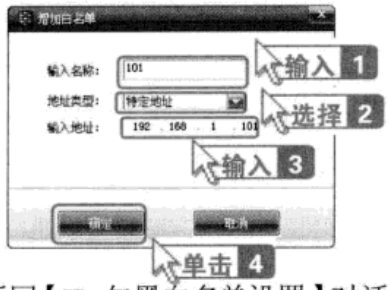
对瑞星防火墙的规则进行适当的设置，能够提高防火墙的拦截效率，更好地保护电脑的安全。设置规则的具体步骤如下。

步骤1 打开瑞星个人防火墙主窗口，单击右上角的【设置】链接，弹出【瑞星个人防火墙设置】对话框，在左侧窗格中展开【网络监控】➤【IP包过滤】选项，右侧窗格中显示瑞星防火墙当前过滤的IP地址，单击右侧窗格中的 黑白名单设置 按钮。

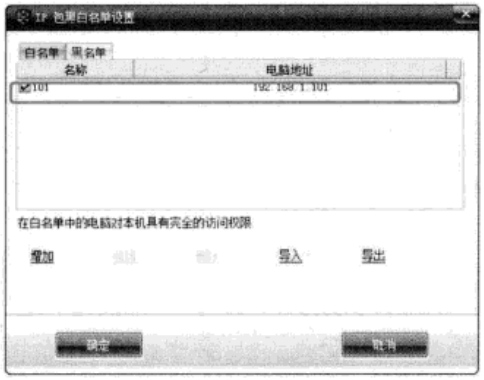

步骤2 弹出【IP 包黑白名单设置】对话框，自动切换到【白名单】选项卡，单击窗口中的【增加】链接。




步骤3 弹出【增加白名单】对话框，在【输入名称】文本框中输入要增加的用户的名称，在【地址类型】下拉列表中选择一种地址类型，选择完成后在【输入地址文本框】中输入要增加用户的IP地址，然后单击 确定 按钮。

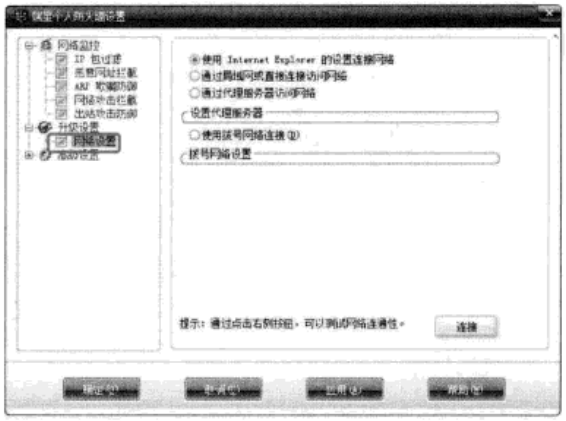



步骤4 返回【IP 包黑白名单设置】对话框，在列表框中即可看到新增加的用户。




步骤5 切换到【黑名单】选项卡，按照同样的方法添加黑名单用户，添加完毕单击 确定 按钮，弹出【确认验证码】对话框，在【请输入验证码】文本框中输入验证码，然后单击 确定 按钮，返回【瑞星个人防火墙设置】对话框。


步骤6 在左侧窗格中展开【升级设置】➢【网络设置】选项，进入【升级设置】界面，用户可以从中设置升级的方式。




步骤7 展开【高级设置】➢【软件安全】选项，进入设置【软件安全】界面，选中右侧窗格中的【启用瑞星密码】复选框。


步骤8 弹出【设置密码】对话框，在【输入密码】和【确认密码】文本框中分别输入密码，在【密码应用范围】组合框中选择密码的使用范围，设置完毕单击 确定 按钮即可。


步骤9 返回【瑞星个人防火墙设置】对话框，在左侧的窗格选择【“云安全”（Cloud Security）计划】选项，进入【“云安全”（Cloud Security）计划】对话框，在【请准确填写您的邮箱地址】文本框中输入用户的邮箱地址，设置完毕单击 确定(O) 按钮即可。当瑞星个人防火墙发现可疑文件时就会以邮件的形式发送到用户的邮箱中以便用户查看。


## 新手问题解答

### 如何用组策略禁止使用文件夹选项

在Windows系统中，“文件夹选项”是“资源管理器”中的一个重要的菜单项，通过它可以修改文件的查看方式、编辑文件的打开方式等，所以为了保护自己的各项设置不让他人随意修改，可将此菜单删除。

选择【开始】➢【运行】菜单项，在【运行】对话框中，输入“gpedit.msc”，按下【Enter】键启动本地组策略编辑器。

在【本地组策略编辑器】窗口中，依次展开【用户设置】➢【管理模板】➢【Windows组件】➢【Windows资源管理器】选项，接着双击右侧的“从工具菜单删除文件夹选项菜单”，在弹出的对话框中选中【启用】单选按钮即可。

### 如何禁止访问“控制面板”

如果用户不希望其他用户访问计算机的“控制面板”，需要选择【开始】➢【运行】菜单项，在【运行】对话框中，输入“gpedit.msc”，按下【Enter】键启动本地组策略编辑器。

打开【本地组策略编辑器】窗口，在左侧的窗格中逐级展开【用户设置】➢【管理模板】➢

【控制面板】选项，然后将右侧窗格中的“禁止访问控制面板”策略启用即可。

此项设置可以防止“控制面板”程序文件（Control.exe）的启动。这样可以使他人无法启动“控制面板”。另外，这个设置将从“开始”菜单中删除“控制面板”，同时还会从Windows资源管理器中删除“控制面板”文件夹。